User Choices and Regret: Understanding Users' Decision Process about Consensually Acquired Spyware

NATHANIEL GOOD, JENS GROSSKLAGS, DAVID THAW,
AARON PERZANOWSKI, DEIRDRE MULLIGAN, JOSEPH KONSTAN*

ABSTRACT

Spyware is software which monitors user actions, gathers personal data, and/or displays advertisements to users. While some spyware is installed surreptitiously, a surprising amount is installed on users' computers with their active participation. In some cases, users agree to accept spyware as part of a software bundle as a cost associated with gaining functionality they desire. In many other cases, however, users are unaware that they installed spyware, or of the consequences of that installation. This lack of awareness occurs even when the functioning of the spyware is explicitly declared in the end user license agreement (EULA). We argue and demonstrate that poor interface design contributes to the difficulty end users experience when trying to manage their computing environment. This paper reviews the legal, technical, and design issues related to the installation of spyware bundled with other software. It reports on results of an experiment in which thirty-one users were asked to configure computers, deciding which software to install from a set of software that included disclosed spyware. The results suggest that current EULA interfaces do little to encourage informed decision-making and that simpler interfaces with key terms highlighted have potential to improve informed decision-making.

I. INTRODUCTION

Over the past several years spyware has emerged as a significant new threat to Internet-connected computers. We use the term "spyware" to describe a class of software that resides on an individual's computer, using the resources of that computer to monitor the user's actions, display advertisements to the user, and/or engage in other activities commonly perceived by users as invasive or

---

* Nathaniel Good, Jens Gossklags, and David Thaw are all at the School of Information Science at the University of California – Berkley. Aaron Perzanowski and Deidre Mulligan are at the Samuelson Law, Technology & Public Policy Clinic, Boalt School of Law, University of California – Berkley and Joseph Konstan is in the Department of Computer Science at the University of Minnesota.

undesirable. Amazingly, these types of programs may reside on up to 88% of all internet-connected computers [5].

Spyware and tools for managing it highlight an interesting junction of legal, technical, and HCI (human-computer interaction) research. While some spyware is installed unknowingly by users when they install freeware or shareware, or when they execute downloads transmitted through email, the web, or instant messages, much spyware is installed *with the user's participation*—it is installed during a software installation process that is apparent to the user and during which the program's actions including spyware behaviors are disclosed. Indeed, the reason that spyware is difficult to accurately define is that the same piece of software may be considered unacceptable spyware by one user, an acceptable trade for other services by another, or a valuable personalization system or notifier by a third. Consider Google's Toolbar (toolbar.google.com) which explicitly asks for permission to monitor user web browsing so that it can provide more information to the user about the page being viewed.

Because of this user-centered definition of what constitutes spyware, for some portion of software that meets the definition of spyware, it seems inappropriate to adopt an outright ban. Early efforts to combat spyware—much like anti-virus software efforts—measured their success based on how infrequently the software was installed. While such a measure can help provide security, it may also limit users access to certain software combinations by denying them the opportunity to trade some privacy, speed, or attention for services or information they actually value. Imagine if your computer "protected" you by preventing you from ever transmitting your credit card information over the Internet; it would perhaps reduce your vulnerability to identity theft, but would at the same time deny you the benefits of shopping online. In the case of spyware, it isn't simply that the monitoring or notifications themselves may be valuable. Anecdotal evidence suggests, and our study confirms, that some users are willing to install spyware when the desired application with which it is bundled is of perceived high utility, and a comparable product without spyware is unavailable or unknown to the user [9]. In other words, at least in situations where users are unaware of other options, they are willing to give up some privacy, screenspace, or bandwidth as "payment" for an unrelated service or product they value.

Accordingly, managing spyware requires that we engage the user in controlling their desktop instead of assuming we can simply do it for them. The End User Licensing Agreement, Terms of Service, Privacy Policy, or some combination (EULA herein) is the most common format for disclosing information about software behavior.

EULAs fail to engage users in the process of controlling the security and privacy settings of their computers, perhaps intentionally. Substantial evidence demonstrates that users rarely read long legal documents—such as EULAs—particularly when displayed in small windows and in a manner that interrupts the installation process. Providing information and requiring the user to acknowledge its receipt prior to installation appears to be the correct approach for several reasons (including the difficulty of uninstalling software programs), but current EULAs, driven largely by legal concerns, do not foster end user control over the desktop. Users typically either do not read or do not understand EULAs. In addition, businesses, and to a lesser extent other end users, are paying dearly for the proliferation of spyware. Equipment and service providers both handle an increasingly high level of customer complaints and customer service calls based on spyware.

In software installation decisions, informed consent is a problem in human-computer interaction, and specifically a problem in interface and interaction design, that should not be left solely to the lawyers.

This paper first provides an overview of the legal, technical, and design issues involved in helping users manage spyware that is disclosed in EULAs. This overview leads to a discussion of the possible "solution graphs" through which inappropriate spyware can be avoided without preventing users from installing similar software that they value. We then report on the results of a set of experiments in which different installation and consent interfaces were used in an attempt to improve user decision-making and discuss the implications for both design and future research.

II. BACKGROUND

A. DEFINITION OF SPYWARE

A fundamental problem is the lack of a standard definition of spyware. Two particularly contested issues are the range of software behaviors that should be included in the definition and the degree of user consent that is desirable.

First, some prefer a narrow definition that focuses on the surveillance aspects of spyware and its ability to collect, store, and communicate information about users and their behavior. Others use a broad definition that includes adware (software that displays advertising), toolbars, search tools, hijackers (software that redirects web traffic or replaces web content with unexpected or unwanted content), and dialers (programs that redirect a computer or a modem to

dial a toll phone number). Definitions for spyware also include hacker tools for remote access and administration, keylogging, and cracking passwords.

Second, there is limited agreement on the *legitimacy* of software that engages in behavior such as targeting advertisements and installing programs on user machines that collect click stream data. Users consider a wide range of programs that present spyware-like functionality unacceptable. However, spyware-like functionality may be acceptable, even desired, in some contexts but objectionable in others (e.g., keylogging as a parental control tool v. keylogging software installed on an adult's private computer without consent). At times the boundary between spyware and legitimate data collection or advertising practice hinges on whether the user is a willing participant in the activity. For example, some personalization features require detailed monitoring of end user interaction with software and/or web content. Where the functionality provided by the software is desired, and the user has actively chosen to allow data to be collected and used for the purpose of personalization, privacy grounds for intervening in the transaction on behalf of the individual are some what diminished. Although the effects of spyware on third parties and doubts about the ability of end users to fully understand the consequences of their decision to allow data collection (for example, a subpoena for their search terms), may support legal intervention even where spyware behavior is agreeable to the end user at the point of software installation. The practice of *bundling* software, which merges spyware with unrelated programs, heightens concerns with the ability of end users to comprehend the ramifications of data collection and advertising practices. Thus, providing another rationale for advocating interventions in private decisions about software installation to protect against externalities that weaken the security of the network overall, and place economic burdens on third parties like service and equipment providers.

In July 2005 the Anti-Spyware Coalition (ASC), a coalition of anti-spyware software companies, academics, and consumer groups, released a document establishing its definition of spyware. The ASC defines spyware as:

> Technologies deployed without appropriate user consent and/or implemented in ways that impair user control over:
>
> Material changes that affect their user experience, privacy, or system security;

> Use of their system resources, including what programs are installed on their computers; and/or
>
> Collection, use, and distribution of their personal or other sensitive information.1

This definition is quite broad including a wide range of software behavior, and hinges in large part on the manner in which the software impairs user control over their computer or engages in behavior without "appropriate user consent." The emergence of a consensus definition is an important step in addressing spyware through technological, market, and regulatory mechanisms.[1] The question of what indicates "appropriate user consent" to permit certain software behaviors is addressed in a second document released in January 2006 by ASC.[2] The ASC Risk Model Description document sets out a series of factors, including notices and control options (opt-out/opt-in) during installation among others, that ASC members consider when determining whether a given piece of software is spyware. Importantly, the document provides insight into the complicated, multi-factor balancing that is conducted by these private companies in determining whether to block, warn users, or allow a software installation to occur.

B. LEGAL ISSUES

Spyware legislation is under consideration in twenty-seven U.S. states and in the U.S. Congress. At least twelve states have enacted spyware legislation. The proposals vary in their focus and scope, ranging from restrictions or prohibitions on unsolicited advertisements, to prohibitions on the unconsented to transmission of personally identifiable information, to requirements that spyware contain removal procedures, to demands on consumer protection agencies to collect complaints. The diversity among state and federal proposals reflects a diverse view of the problem, as well as the

---

[1] Anti-Spyware Coalition, "Anti-Spyware Coalition Definition and Supporting Documents." http://www.antispywarecoalition.org/documents/definitions.htm.

[2] Anti-Spyware Coalition, "Anti-Spyware Coalition Risk Model." http://www.antispywarecoalition.org/documents/RiskModelDescription.htm.

influence of various parties who have supported and opposed spyware legislation.

The spyware provisions that limit or prohibit the collection or transmission of certain personal information without the individual data subject's consent are consistent with general principles of data protection. Europe's data privacy and data protection laws, while not spyware specific, embody this principle. In general, these laws require that information be collected for a lawful and limited purpose, and that individuals consent to the collection of their data, be informed of the use, have the right to inspect and correct such data, and the right to revoke consent in the future. The focus on informed consent in the data protection context, resonates with the ASC's focus on "appropriate user consent" and extended consideration of factors that may evince such consent in the Risk Modeling document.

In the absence of specific spyware statutes, spyware is governed by existing laws governing contracts, fraud, and computer hacking. An examination of the few U.S. cases that directly address spyware shows that the courts place a strong emphasis on the existence of an agreement with the user to install the software.[3] For example, in *Federal Trade Commission v. Seismic Entertainment*,[4] the FTC alleged that the Seismic's software script exploited web browser security vulnerabilities to download and install programs without the computer user's knowledge or authorization. The surreptitiously installed software then served ads promoting Seismic's anti-spyware software. The court found the FTC likely to succeed in a case based on unfair and deceptive acts and practices and granted a temporary restraining order against Seismic.

Given the courts' focus on consent, many spyware programs, particularly those distributed through channels with legitimate reputations, attempt to establish an agreement with the user through a EULA. Software EULAs are governed by traditional contract law. The formation of a legally enforceable agreement requires a concrete offer by one party and clear acceptance of that offer by the second party. Contracts are binding because they represent the parties' mutual

---

[3] New York Attorney General Elliot Spitzer filed charges against Intermix Media for trespass, false advertising, and deceptive business practices. Intermix distributed screensavers and games bundled with spyware. These charges, which were settled before a court decision, stemmed in part from misleading, inaccurate, or nonexistent EULAs.

[4] FTC v. Seismic Entm't Prod's, No. 04-377-JD, 2004 U.S. Dist. LEXIS 22788 (D.N.H. October 21, 2004).

assent to bargained-for terms. This meeting of the minds is central to the legal justification for contract enforcement.

In the software EULA context, the traditional contract paradigm faces difficulties. Most importantly, end users' manifestations of consent are often ambiguous. Some software is governed by terms merely posted to the web page from which the software is downloaded.[5] These browsewrap agreements require no overt act during installation on the part of the end user to demonstrate assent to the EULA terms. Similarly, courts have enforced shrinkwrap agreements that purport to bind users to EULA terms that appear on software packaging simply because the user opened the package.[6]

Even clickwrap agreements, which require users to click the ubiquitous "I Agree" button, pose problems. Often end users fail to understand the purpose or legal significance of EULAs. And, of course, many simply have become conditioned to view them as a meaningless but necessary hurdle in the software installation process. As a result, users often fail to read them. Even those that do read EULAs often find the documents indecipherable because of their length, the format in which they are displayed, and the use of specialized technical and legal language.

If users read and understood the terms of software EULAs, many would be surprised by the number of legal obligations they create. For example, after just a few clicks, a user installing KaZaA agrees to provisions that prohibit reverse engineering, altering registry keys, disabling advertisements, and removing third party software. In addition the user "assents" to no less than three "choice of law" provisions and an arbitration clause. The user indemnifies the software providers for any infringing transmissions and permits the sharing of contact information and browsing history for the purposes of receiving promotional emails and targeted advertisements. The software companies disclaim any warranties and limit their liability for the misuse of personal data or damage to the user's computer. These agreements claim to bind all subsequent users of the software, regardless of their awareness of the EULA terms. While it is certainly likely that *some* users would willingly agree to those terms in order to use KaZaA, we strongly doubt that *all* users who clicked through the KaZaA EULA would have a genuine "meeting of the minds." Indeed,

---

[5] Specht v. AOL, 306 F.3d 17, 22 (2d Cir. 2002).

[6] Bowers v. Baystate Technologies, Inc. , 320 F.3d 1317 (Fed. Cir. 2003).

our results below show that some users regret installing programs like KaZaA after being informed of the contents of the EULA.

Despite the problems EULAs present, courts typically enforce them. Even in more traditional contract contexts, performance of an act can serve as acceptance of a contract. In the EULA context, courts typically find that installing or using the software is sufficient to establish acceptance of EULA terms even when users are not required to click "I Agree."[7] Further, the user's failure to read a EULA rarely mitigates against a conclusion of contract formation. When a document is reasonably understood to create legal obligations, courts impose a duty to read.[8] This obligation to read extends not just to EULAs but to documents hyperlinked from EULAs as well.[9] And while EULA language is far from clear, courts are reluctant to excuse violations on the basis of confusing language.

At the same time, some courts have called into question whether users have agreed to EULA terms. In *Sotelo v. DirectRevenue, LLC*,[10] the court refused to require arbitration, as specified in the EULA, by finding that agreement to the EULA was itself a triable issue of fact. Courts have great latitude in determining whether a contract is in place. They may even refuse to enforce unconscionable contracts, although they rarely do so. Part of the motivation for our research is to provide objective data on whether users understand the nature of their agreement and the terms to which they agree when installing spyware which is disclosed in the software EULA.

C. TECHNICAL ISSUES

While a detailed discussion of technical approaches to addressing spyware goes beyond the scope of this paper, it is important to review the most common solutions in use and to discuss the limitations and potential of these solutions. Dozens of spyware defense software packages focus on scanning a computer to identify and remove suspicious software, registry keys, and files. Others prevent software

---

[7] See Tarra Zynda, Note, *Ticketmaster Corp. v. Tickets.com, Inc.: Preserving Minimum Requirements of Contract on the Internet*, 19 Berkeley Tech. L.J. 495, 504-505 (2004).

[8] Heller Fin., Inc. v. Midwhey Powder Co., 883 F.2d 1286, 1292 (7th Cir. 1989).

[9] Hubbert v. Dell Corp., 835 N.E.2d 113 (Ill. App. Ct. 2005).

[10] Sotelo v. DirectRevenue, LLC, *384 F. Supp. 2d 1219, 1228* (N.D. Ill. 2005).

from making certain system changes (e.g., modifying registry keys or the browser home page).

A smaller number of products protect against leaks of personal information. For example, Norton Internet Security blocks transmission of personal data via web forms, e-mail, instant messenger, etc., without user knowledge or consent. More specific tools such as eBay's toolbar protect against disclosure of particular sorts of data, in this case eBay passwords.

Some argue that instead of designing better notices which consumers will ignore, we should concentrate on designing better technology because in the end, "users just want us to do it all for them." The argument is that users lack the skill, methods, or desire to manage their computer and protect themselves from Spyware and are therefore willing to relinquish this responsibility to a software program or operating system, trusting technological means to handle this effectively. Virus programs were unwanted hosts that were stowaways on legitimate applications, often causing unwanted effects from the benign (displaying short messages or poems like "elk Cloner") to damaging files on the infected host or coordinating massive DDOS attacks on high traffic targets. The industry that sprang up to defeat this threat had one mission, to successfully detect and eliminate these stowaway programs and remove them from their infected applications. The question is, why shouldn't the same be done for Spyware? There are many good reasons why this should happen. Spyware programs, especially those that are more deceptive in nature, require experts to understand their operation and removal. Experts also have the benefit of larger resources and experience, and can make more informed decisions on what is 'good' or 'bad' based on much better data than that available to most users.

Ignoring the technical complications with such an approach, spyware has proven to be a much more complicated problem to eradicate because its definition often turns on the level of user control or "consent" over the software's operation. A majority of computers and most new computers come with some form of Anti-Spyware/Anti-Virus tool, yet spyware remains a large problem.

First there is the issue of how exactly the Anti-Spyware programs operate. Methods of detection, criteria for flagging, and underlying motivations for detection, all present important questions.

There are many Anti-Spyware applications. Generally, they use different detection schemes, different criteria, and even different methods of flagging software. Because the specifics of an anti-spyware program's operation is generally not public, there are some who question the motivations of the anti-spyware vendors. Recently,

companies such as Microsoft have come under fire for changing how they flag certain programs. The argument is that because these criteria are not standard and open, there is always a risk that companies may choose what to flag and not to flag based not on customers' best interest, but that of the anti-spyware vendor. The ASC documents described above in conjunction with the ASC "Vendor Dispute and False Positive Resolution" document, provide some understanding of how anti-spyware vendors make decisions about what software to block or label and provide procedural protections to software vendors who believe they have been unfairly dealt with.

In addition to suspicion from some consumer activists, anti-spyware companies also routinely come under fire from vendors that they tag as spyware as well. Some vendors have even filed lawsuits, and used other methods to push anti-spyware vendors to re-evaluate or downgrade their products. While well defined criteria may help alleviate this problem, the ultimate decision is up to the consumer. If consumers are provided an adequate means of evaluating the criteria for themselves, then the anti-spyware vendor has a much easier job concentrating on removing items that are clearly bad, and passing the hard, context dependent, decisions on software in the grey areas to consumers themselves.

At present, there are two major weaknesses that prevent anti-spyware tools from forming a complete solution. First, the tools themselves are incapable of catching or removing all known spyware (let alone unknown spyware). Second, the tools are not (and perhaps cannot be) sophisticated enough to understand a given user's trade-offs between privacy, system performance, security and the functionality enabled by a product. While limiting the scope in which the tool is deployed can limit the choices users will have to make (corporate environment vs. consumer machine), even if the tool can identify a potential privacy or security threat, it is necessary in many cases to present that threat to the user for the final decision about installation.

Currently, the burden of informing the users falls on the EULA. For these reasons, in addition to good software tools and operating system design, it is important that we consider what user interface design methods in conjunction with what legal reforms could improve the current state of software disclosures and ultimately improve an end users ability to successfully manage their computer environment.

D. Privacy Attitudes and User Behavior

Consumers often lack knowledge about risks and modes of technical and legal protection [3]. For example, a recent AOL/NSCA study showed that users are unaware of the amount of spyware installed on their computers and its origin [5]. A related study on the use of filesharing clients shows that users are often unaware that they are sharing sensitive information with other users [23].

Users also differ in their level of privacy sensitivity. Westin [6] found that consumers fall generally into one of three categories: privacy fundamentalists, privacy pragmatists, and the marginally concerned. Other research shows that the pragmatic group's attitudes differ towards the collection of personally identifying information and information to create non-identifying user profiles [23] and can be distinguished with respect to concern towards offline and online identity [3]. Users also show great concern towards bundling practices and the involvement of third parties in a transaction [3][12].

Experimental research demonstrates that user behavior does not always align with stated privacy preferences [3][23]. Users are willing to trade off their privacy and/or security for small monetary gains (e.g., a free program) or product recommendations [3][23]. Moreover, Acquisti and Grossklags [3] report evidence that users are more likely to discount future privacy/security losses if presented with an immediate discount on a product. Consumers may also accept offers more often when benefits and costs are difficult to compare and descriptions are provided in ambiguous and uncertain terms [4].

E. Online Privacy Notices

EULAs, ToS, and some privacy policies present complex legal information. Research shows, however, that complexity of notices hampers users' ability to understand such agreements. For example, Jensen and Pott [15] studied a sample of 64 privacy policies from high traffic and health care websites. They found that policies' format, location on the website and legal content severely limit users' ability to make informed decisions.

One attempt to improve users' ability to make informed decisions is the Platform for Privacy Preferences Project (P3P) [23]. Under this standard, websites' policies are expressed in a predefined grammar and vocabulary. Ackerman and Cranor [2] explored ways to provide user assistance in negotiating privacy policies using semi-autonomous agents to interact with P3P enabled sites. Another system [11] encourages users to create several P3P-enabled identity profiles to

address information usage patterns and privacy concerns for different types of online interactions. However, [25] Vila et al. raise the question of whether users will ever be bothered to believe or read privacy policies at all. They claim that because the cost of lying in a privacy policy is low, and that some of the privacy policies are not trustworthy, users do not feel it is worth their time to read them or pay attention to them at all. The fact that EULAs can change their terms at will further reduce users incentive to pay attention to them.

F. MULTI-LAYERED NOTICES

Research on product labeling and hazard warnings (see, for example, [21]) focuses on improving the efficiency of consumer notification.[11] This research has influenced the formulation of different methods for presenting notice to the end user. For example, researchers from the Center for Information Policy Leadership call for statements in short, everyday language that are available in a common easy-to-read format[12]. However, they also caution that legal requirements require companies to provide complete notices that do not fit this standard (see, for example, [1]). They propose a *multi-layered notice* with a minimum of two notices that first provide a summary at the top level, increasing detail at the lower layers, and the complete, detailed notice as a final layer. The layering should include a *short notice* (also called condensed notice or highlights) that provides the most important information in a consistent format, including the parties involved, contact information, and the type of data collected, and the uses for which it is intended.

There is varying governmental support for layered notices. For example, the European Union has taken concrete steps towards a

---

[11] The debate over labeling and notice is also taking place in the area of Digital Rights Management (DRM). DRM systems limit a consumer's ability to share copyright protected content through digital media software and hardware features. Users implicitly agree to these limits when purchasing DRM equipped products. Some consumer advocates believe this kind of implicit notice is not adequate to alert consumers to the reduced functionality of the product they are purchasing. In 2003 Reps Boucher (D-VA), Lofgren (D-CA) and Brownback (R-KS) introduced the Consumers, Schools and Libraries Digital Rights Management Awareness Act which attempted to increase consumer DRM rights.

[12] P3P clearly shares the same goals, however, with a somewhat complementary solution process.

layered notice model.[13] In the United States, the Department of Health and Human Services has encouraged entities covered by the Health Insurance Portability and Accountability Act (HIPAA) to prepare such notices [20]. In addition, currently proposed Spyware legislation asks that companies provide notices in an easy to process format. However, despite public consideration[14], there is no broad consensus for the financial industry pursuant to the Gramm-Leach-Bliley Act [1].

G. HCI AND DESIGN ISSUES

Our research shows that software EULAs are not an effective mechanism for conveying information to end users. Through interfaces that, increase awareness of significant issues, we may create greater potential for informed consent. However, HCI is only a partial solution.

The challenge of attracting attention to important events is not a new one in HCI. A number of researchers are studying the effects of notification systems in computing. Examples of systems include instant messaging, user status updates, email alerts, and news and stock tickers. This research examines the nature of interruptions and people's cognitive responses to work-disruptive influences. Notification systems commonly use visualization techniques to increase information availability while limiting loss of users' focus on primary tasks [6][14][27]. From control room and cockpit indicators to desktop notifiers, substantial research has been devoted to identifying visual and auditory displays that attract attention and to designing interaction sequences that prevent automatic dismissal of information.

As a trivial example, it is now somewhat common to prohibit the use of an "Agree" button until after the user has viewed the entire agreement. Of course, scrolling to the end of the agreement defeats that simple intervention.

---

[13] Article 29 Data Working Party, "Opinion on More Harmonised Information Provisions," http://www.datenschutz-berlin.de/doc/eu/gruppe29/wp100/wp100_en.pdf. The Article 29 Data Protection Working Party is an independent advisory body set up under Article 29 of Directive 95/46/EC, and it outlined this approach.

[14] See Federal Trade Commission. Getting noticed: writing effective financial privacy notices. http://www.ftc.gov/bcp/conline/pubs/buspubs/getnoticed.pdf. (notes from a public workshop discussing how to provide effective notice under the GLB Act: Get Noticed: Effective Financial Privacy Notices, (Dec. 4 2001)).

If the particularly relevant terms or conditions of a EULA can be identified, it is possible to summarize them in a short, easy-to-read form. If standardized agreements are designed, it is possible to highlight only unusual terms. For example, the European Union's approach to consumer protection in standard mass-market consumer contracts, such as EULAs, pursues a mixture of standard terms and construction presumptions against non-standard terms. Below we experiment with interfaces that use such a design to determine how effectively they can change user actions and user satisfaction with their software installation decisions.

Given the variety of individual preferences, it may be necessary to develop a profile of preferences (much like P3P for web-based privacy) to alert users to cases where an agreement or a software system may be traversing their usual preferences. The success of any such notification system depends upon both the reliability with which such determinations can be made and the number of false positives—the number of alerts that the user chooses to dismiss rather than honor. We have all become accustomed to web browser alerts (e.g., for moving from a secure to insecure site) that are not sufficiently valued and are therefore turned off.

In sum, user interface design alone will not afford end users with adequate information and control over software behavior. While the lessons of HCI can help inform the presentation of information to users, the technical and legal underpinnings are essential to avoid carefully presenting the user with little more than noise, or worse, creating a "usable" privacy or security solution in which users can simply, efficiently, and more knowingly undermine their privacy, security, or other interests.

III. SOLUTION GRAPHS

We refer to the ideas in this section as solution graphs because they flow from the analysis illustrated in figure 1. The goal of this section is to identify a set of partial solutions, and to identify a set of research questions that can help inform us as we pursue these questions.

Spyware is not a clean category, but rather a fuzzy one. Nonetheless, for some set of spyware, it may be that an authority determines that it should be prohibited. That authority may be legal (e.g., banning the transmission of Social Security numbers through such software), or more likely organizational (e.g., a company determining that any software in certain categories is banned). The first solution graph, therefore, is a legal/technical one. If the authority

is governmental, such software may be prohibited by law. Whether governmental or organizational, such software may be prevented or removed by anti-spyware tools. This solution bypasses the entire question of informed consent by declaring that the user's opinion of the software is inconsequential.

If the software is not banned or blocked, then the decision of whether to install it should be left to the user. One would hope for an honest and accurate disclosure of the functioning of the software; however the current state of consumer protection law creates perverse incentives that can discourage disclosure. An inaccurate disclosure is more likely to create liability than a lack of disclosure. Therefore entities that provide more detailed notices and explicit promises to consumers risk faces greater legal exposure for divergent practices than those who remain silent. Today there is a lack of incentive to provide complete and accurate disclosures. There is growing pressure on spyware companies, particularly adware companies, to use EULAs to describe software behavior. While these incentives may drive legitimate businesses they are unlikely to influence the behavior of truly egregious actors.

Unsurprisingly, given the state of EULAs, users may be skeptical of company disclosures and turn to trusted third parties such as anti-spyware companies to assess the software's behavior. One could imagine a light weight service that served a *Consumer Reports* function, rating or scoring software to summarize their assessment of the risks and trade-offs involved in its installation and use.

Assuming, for purposes of this section, there is a full and accurate disclosure, the next question is whether there is a meeting of the minds—informed consent. As we show below and others have shown before, EULAs are not well suited to provide information to users or to aiding user comprehension. There exist several challenges to informed consent: 1) the consent process appears as an obstacle on the way to a task; 2) the length and language of documents used to convey information to users; and 3) the triviality of the consent mechanisms employed ("I agree"). Consider spyware installed with a game downloaded from a web site. The user eager to play this game is unlikely to break concentration from the task to give serious time and consideration to the consequences, particularly if doing so requires reading a multi page document containing dense legal and technical language. One solution to this dilemma would be to delay gratification—if software installation did not take effect for some period of time then users might have time to reconsider their actions. This "cold shower" approach has been incorporated in law to protect consumers in potentially high-pressure, high-stakes contexts (such as

in-home sales). Early results in computer-based education show some promise: when users were not allowed to respond immediately to questions their answers improved.

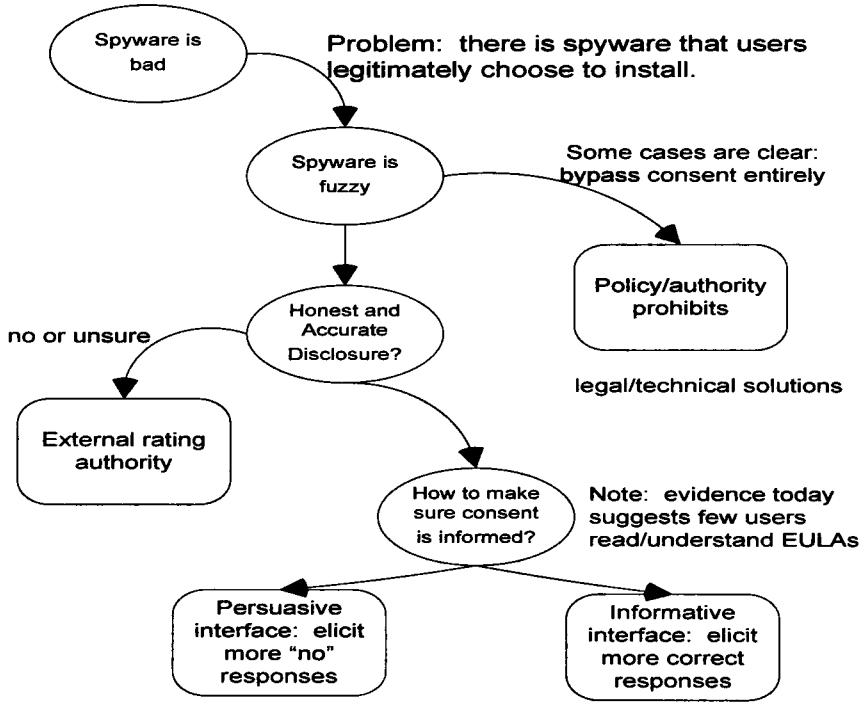


Figure 1: Graph of possible solutions to spyware problem

Since most users are unlikely to agree to a waiting period before software installation, the remaining choices are all about the user interface. Here, there have been two directions. Persuasive approaches have been used to elicit a predefined correct answer more often. For example, warning people that untrusted software can damage your computer attempts to elicit a "no" response. Informative approaches can be measured on their effectiveness in getting users to give the correct answer, whether that answer is "yes" or "no." Such approaches may include summaries of terms, matches between terms and profiles, and even a clear statement of costs and benefits.

We argue that the nature of spyware today requires the union of these techniques. Realistically, individual informed consent is an attention- and effort-intensive process. Individuals need the backup of legal infrastructure to prohibit the most egregious offenses, to force

the honest disclosure of terms and effects, and to protect them against over-reaching and unconscionable terms. Technology can help enforce preferences when they can be accurately expressed and their violation detected. External agencies can help by providing ratings of risk and quality. But in the end, users must have the control to make certain decisions about trade-offs between their privacy, their security, their attention, and the services or products they desire.

In the rest of this paper, we describe an experiment on different notice conditions, describe the results, and explore a set of questions to help us along the way towards an environment in which meaningful, informed consent is more likely to be achieved.

IV. Experimental Design

We conducted a study in which participants were being observed while they considered installing five real world applications. Our goal was to examine the factors that contribute to users' application choices when those programs exhibit behaviors that can harm their information privacy, computer security, and system performance. In particular, we aimed to understand what impact currently implemented and proposed warnings and notices have on users' installation decisions of potentially harmful software and their knowledge of likely privacy and security consequences.

The goals of our investigation required us to study not only quantitative data about installation frequencies but also qualitative data about subjects' impressions of the programs under consideration close to decision time. We, therefore, opted for direct observation of each individual followed by an in-depth interview process that also included brief surveys on attitudes towards program behaviors and individuals' knowledge with respect to computer configuration tasks.

Alternative study designs would have allowed for collection of different types of data.

One alternative design would be to record users' actions on their own machines over some period of time and ask users questions about the types of programs they installed. However, this approach is error-prone, as it depends upon users correctly remembering and commenting on their actions.

A long-term log or a one-time audit of user machines, as conducted in the Earthlink spyware study [12], would have permitted us to record the number of potentially harmful programs on users' computers. However, it would not have provided a way to study individuals' behavior during the program selection and installation process.

To gain a better understanding of users' behavior, we needed to observe the process and ask the users questions immediately after the experiment was performed. While the trade-off of this approach is fewer users than a survey or audit study, the advantages of the study approach is that we were able to obtain sufficient data, observe all interactions with the software, gather qualitative data about the decision-making process during and after installation, and maintain consistency across subjects.

A drawback of our approach is the small number of participants that limits our ability to present statistically robust results. However, we believe that our exploratory study helps to provide a good overview of the multi-dimensional information gathering and choice process of individuals that would not have been possible with a more constrained study methodology. We suggest that our study provides enough data to inform and guide our further experimentation into user behavior and notice design.

A. EXPERIMENT CONSTRUCTION

1. APPLICATIONS USED IN THE EXPERIMENT

As part of our study, we selected five applications that users could download. Each contained bundled software or functionality that monitored user's actions or displayed adds. The criteria we used in selecting our programs were:

1. The program must have a legitimate and desirable function;

2. The program must have some type of bundled functionality that could be averse to a given user's privacy/security preferences; and

3. Programs must display a notice of terms (EULA, ToS/ToU) that aim to contractually bind the user upon installation.

We chose the following programs:

- KaZaA – "A peer-to-peer file-sharing program that allows you to share and download media files from other users."

- Edonkey – "A peer-to-peer file-sharing program that allows you to share and download media files from other users."

- Webshots – "This program provides a variety of ways to use photos for your computer desktop as wallpaper and screensavers."

- Weatherscope – "A program that displays your current local temperature whenever you are online. It provides one-click access to 3-day and 7-day forecasts."

- Google Toolbar – "A program that allows you to search the web from any web site, eliminate pop-up ads and fill in forms with one click."

We wanted the programs to reflect the range of behavior and functionalities that users encounter while installing applications in the real world. We selected some programs that had explicit opt-out options (e.g., Google Toolbar and Edonkey) and some that lacked such options (e.g., KaZaA and Weatherscope). In addition, we included programs that bundled multiple seemingly unrelated applications (e.g., KaZaA) and a program that likely does not bundle additional software or functionality (e.g., Webshots).

During our selection process we aimed to include programs with different brand reputation. For this reason, we chose a program from a brand with a positive association, such as Google. Other programs in our study received substantial negative press, such as KaZaA.

Importantly, while these applications include or bundle program behaviors that may conflict with users' privacy and security preferences, we did not suggest to participants that any of them contain spyware. Perception concerning each programs' behaviors, and disclosure and consent procedures often decide whether a program is considered spyware or not, both by end users and by anti-spyware vendors. Therefore, our research intentionally included software that users would unlikely consider to be spyware or even intrusive (e.g., Google Toolbar).

2. EXPERIMENT SCENARIO

In order to motivate our users to make a decision to install or not install a given program, we created a scenario for users to follow. We wanted to provide users with a reason to consider installing some or all of the programs, but we also wanted to ensure that they were not obligated to install any of them. We thus presented the user with the following situational description:

Imagine that a friend (or relative) has asked you to help set up this computer. The computer already has the most popular office applications installed. Your friend wants additional functionality and is considering installing other software.

Here is a quote from your friend: "Here are some programs that were recommended to me by my friends. Since you know more about computers than me, can you install the ones you think are appropriate?"

The five program executables were located on the desktop of the computer used by the participants. The displayed name of the executables as well as the study instructions did not reveal the programs' brands or names. They were referred to as Program A, B, C, D and E. Subjects, however, received basic descriptions of the programs below the printed scenario description in the instructions. For example, we described KaZaA and EDonkey as: "Program A (or E) - A peer-to-peer file-sharing program that allows you to share and download media files from other users." For each study subject we randomized the arrangement of the programs in the instructions and on the desktop to avoid order effects.

If users decided to install a program, they could double click on the program's installation icon which started each program's standard installation routine. They could decide at any time to cancel the installation and go on to the next program.

3. NOTICE CONDITIONS

We wished to examine whether different types of notices would affect a user's decision to install a program. We were also interested in capturing if users were aware of each type of notice, and their recall of the notice after installation. We chose three different types of notices. Below we describe the characteristics of each notice condition.

Notice Condition 1 - EULA Only: The first notice condition is a control treatment consisting of only the original EULAs and notices

that are included in each program. This notice condition represents what most users would see when they install a program downloaded from the internet.

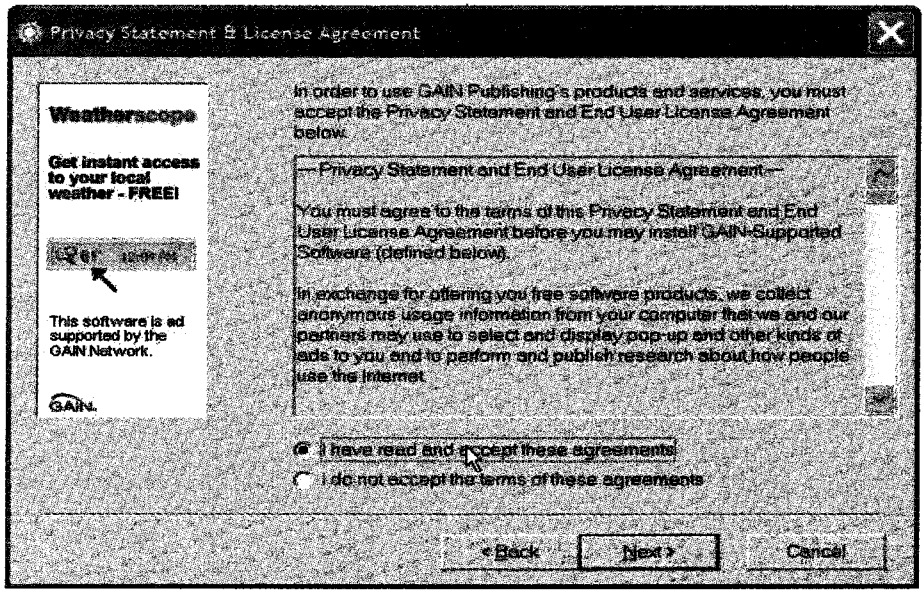


Figure 2: EULA for Webshots

Notice Condition 2 - Microsoft SP2 Short Notice + EULA: In addition to the EULA included in each individual program, the second notice condition includes a short warning from Microsoft that is displayed when users begin the installation. This warning is included with Windows XP Service Pack 2, and is provided for all programs that are downloaded from the web. If available, the notification includes a link to the publisher information as well as links to privacy policy information. The purpose of this notice condition is to test if a commonplace heightened-notice practice, active by default, will affect installation behavior.

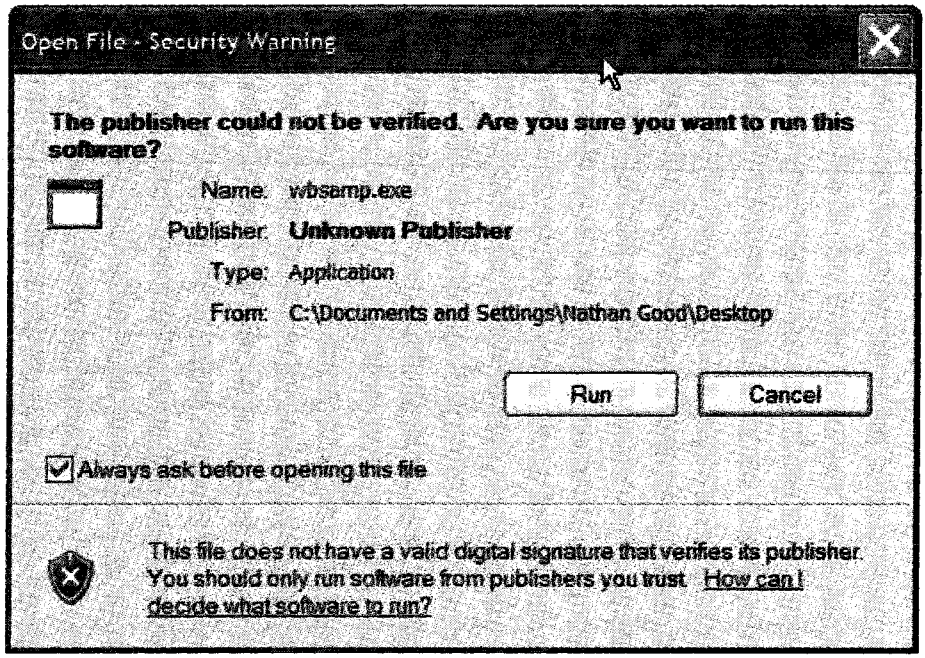


Figure 3: Microsoft Windows XP SP2 Warning

Notice Condition 3 - Customized Short Notice + EULA: The third notice condition consists of a layered notice: a customized short notice in addition to the EULA included in each individual program. In this notice condition, the short Microsoft warnings shown in notice condition 2 were disabled. Users were instead presented with a window that provides specific information about each program (see Figure 3). When users reached the portion of the installation program that showed the EULA, this window appeared in the forefront of the EULA automatically. We describe how we decided on the content and presentation of these short notices in more detail below.

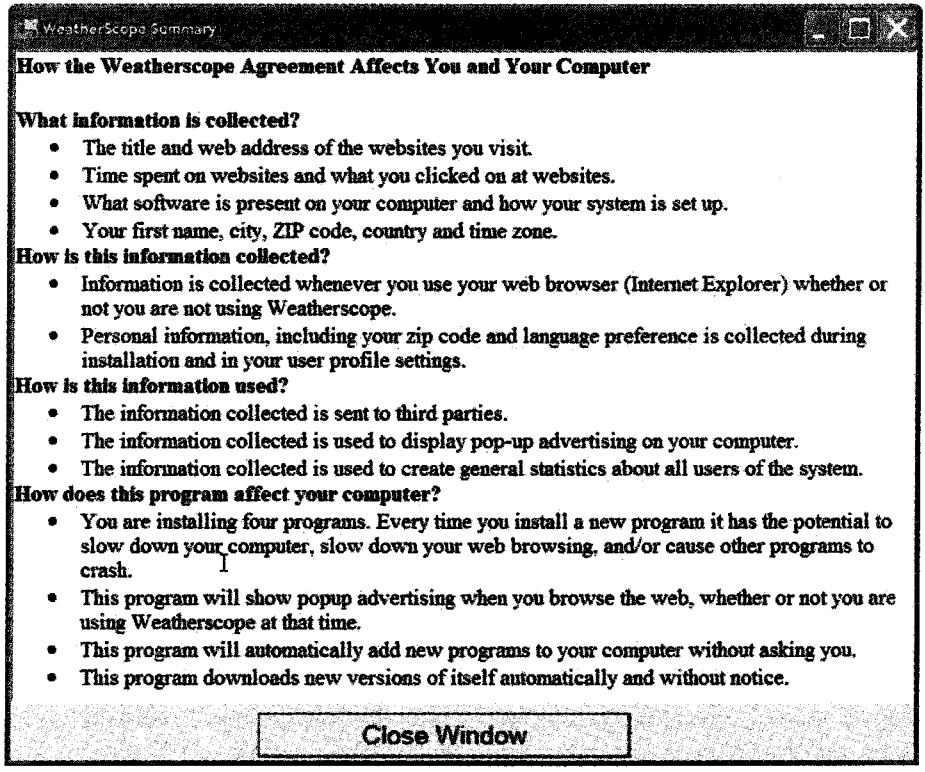


Figure 4: WeatherScope Customized Short Notice

4. CREATING THE SHORT NOTICES

As noted above, there exists considerable legal and computer security literature that deals with short notices. The actual content that a short notice should contain is slightly different in each proposal, but they all recommend that the most relevant information should be presented clearly and concisely. The EU model suggests that the condensed notice should contain all the relevant information to ensure people are well-informed about their rights and choices.[15] The key points of a short notice are that they should use language and layout that are easy to understand, and they should include:

---

[15] Article 29 Data Working Party, "Opinion on More Harmonised Information Provision," http://www.datenschutz-berlin.de/doc/eu/gruppe29/wp100/wp100_en.pdf.

- The name of the company
- The purpose of the data processing
- The recipients or categories of recipients of the data
- Whether replies to questions are obligatory or voluntary, as well as the possible consequences of failure to reply
- The possibility of transfer to third parties
- The right to access, to rectify, and oppose

The purpose of our study is neither to create a new standard for short notices, nor to evaluate the effectiveness of various language terms. Rather, our goal is to determine if any short notice would have an effect on a user's installation decisions. For this reason, we chose to emphasize the aspects of a EULA that were consistent with users' expressed privacy/security preferences, such as items describing third party access to information and the impact on machine performance (slow down, crashing, popups, etc.). We borrowed heavily from existing recommendations when appropriate, using a simple layout, bullet points, and easy to understand language. We created a series of four generic privacy/security questions, which we answered for each program in the notice. An example short notice is shown in Figure 4.

We derived the content for each short notice by examining the TOS and EULA for each program, and answered each of the four questions described below using consistent language across notices. Our aim was to include information that those skilled in the art would know or be able to infer about the program by installing it.

We aimed to answer the following questions in a consistent fashion across programs:

- **What information is collected?** The purpose of this question is to describe in common language what information is being collected by the program. This is in keeping with the proposals of the EU and P3P notices.
- **How is this information collected?** The purpose of this question is to inform users how the information

above will be collected by the program being installed and all of its additional components.

- **How is this information used?** The purpose of this question is to provide information to users about how the program and its additional components will use the information collected (above). If information is given to third-parties, such would be noted here.

- **How does this installation affect your computer?** Users are often concerned about system performance issues that may arise when they are installing new software. In many cases, this may be the most important factor in deciding whether to install a program. Measuring operating system impact in relation to other programs the user may have already installed and their current configuration is non-trivial. Ideally, it would be nice to say "the computer will be 25% slower" or "it will take an extra couple of minutes to perform common tasks," yet the complexities and unknowns of various configurations makes it difficult to do so. We instead opted for an approach that would educate users about the possible consequence of installing additional programs. For this reason, we chose to tell users the number of programs they were installing, and that additional programs could cause the computer to behave more unreliably and possibly slower.

Information about uninstalling programs is also important to users. However, we chose not to include this in our short descriptions since it is difficult to articulate the degree of difficulty to remove a program, and we lacked detailed technical information about each individual program to determine what is actually removed by uninstalling the program. However, we thought it would be valuable to capture user capabilities in detecting and uninstalling software using common Microsoft Windows tools. Therefore, we included related questions in a post-installation survey. In future work, we will look more closely at user behavior in the uninstall process.

5. SURVEYS AND POST STUDY INTERVIEW

During the experimental phase we anticipated users to be influenced by a multitude of individual preferences and strategies that would contribute to their decisions to gather different degrees of information about a program and finally to install or not to install a program. For example, some participants might have a positive prior experience with a program, while others are not interested in a program's functionality. To gain greater insight into these unobservable factors and the causes for users' behaviors, we involved each user into a post-experimental standardized open-ended interview [18] with two nested one-page paper surveys. We created an interview script with a set of carefully worded questions and transitions as well as with a fixed ordering aimed to create a comparable experience for all participants. We indicated opportunities for probing users' responses and included certain suggestions for brief follow-up questions in the script. For treatments 2 and 3, we added a brief section to study the specific effects of these treatments but otherwise kept the survey unchanged. We attempted to place this additional section so that the perceived difference between the interviews would be limited. The interviews were planned to last for an average of 45 minutes, and actually took between 35 and 60 minutes.

We structured the interview into the following sections:

1. Basic Demographic Information
2. Reasons for Install/Uninstall of each program
3. Ask for recommendations how they would change the installation process to assist in decision making process
4. Prior Experience with Programs
5. Questions about Notice and Contractual Agreements (Added specific questions about notice conditions 2 and 3)
6. First Survey on privacy preferences
7. Reaction to Short EULAs, determine if they regret the decision to install/ not install

8. Ask again for recommendations to installation process to assist in their decision making process

9. Second survey on technical capabilities

10. General comments and feedback to our study

Section I included questions about participants' age and computer usage practices. Then, in section II, we studied participants' reasons that motivated them to install or not install each program. First, for each program installed by the participant, we queried for her reasons to act in this way, and followed up with a question asking whether she had also considered any factors for not installing the program. Second, we continued this section discussing programs that were not installed by the participant reversing the order of these two questions. In section III we asked whether any (unspecified) factors with respect to the installation screens helped users in their choice to install or not, succeeded by a generic question whether participants would recommend any improvements to those screens to help them with their installation decisions. By starting with these very basic questions, in sections II and III, we aimed to derive a general understanding about participants' motivational drivers for their program choices before we would involve them into a more focused dialogue on the notice conditions. At this point, we expected that participants would more likely refer to security concerns in conditions 2 and 3 compared to the control condition 1.

Section IV investigated participants' prior knowledge of each program: did they hear of it; did they install it themselves; and did they actually use it. Next, in section V, we investigated whether participants were aware that by installing a program they entered into a contractual agreement with the software producer, whether they remembered anything about those agreements, and whether this information had any impact on their installation decisions. At this point we also inserted questions about notice conditions 2 and 3.

Then, in section VI, we presented participants with a paper survey that listed sixteen program features: some being likely undesirable and commonly associated with spyware, and others that we considered as potentially beneficial. Participants indicated their level of concern with those features on a 5-point Likert Scale (with 1: 'not concerned;' 5: 'extremely concerned'). In section VII, we asked participants to study the short notices for each program. We requested participants to revisit their earlier choices to install or not install each program, and what information in the short notices could contribute to change their

mind or not.[16] We anticipated participants to show different types of reaction (e.g., regret or confirmation of their earlier decisions) depending on, for example, their prior knowledge of the program and their attitudes towards the features listed in the short notices. Subsequently, in section VIII, we asked participants to reconsider whether they would desire any changes to the installation process of the programs provided. We note that sections II-III and VII-VIII are not redundant for notice condition 3, since we could not foresee how each participant would react to the short notices during the experiment (e.g., some would study them carefully, while others would ignore them).

In section IX participants were asked to indicate their level of comfort and prior experience with thirteen computer maintenance practices commonly connected to defending against, and removing spyware (e.g., configuring a firewall and editing the Windows registry). The survey format facilitated a response on a 4-point scale (ranging from 'not comfortable at all' to 'have done this many times;' we also gave participants the option to indicate that they are 'unsure'). We concluded in section X by asking for general comments about our study.

We should note that the purpose of the nested surveys was not to create broad generalizations of the computing public at large. There have been many other surveys that have provided excellent data on users' privacy and security preferences. Rather, our surveys were included to get a better understanding of our subjects' capabilities and concerns, and to use this information to guide our questions and analysis, as well as to tie back our results to the larger research community.

V. RESULTS

A. PARTICIPANT DEMOGRAPHICS

Our user sample consisted of 31 participants: 14 male and 17 female university undergraduates assembled by a university recruiting service. All used the Windows operating system on their home computer, and 24 of them maintained their computer at home

---

[16] For participants that experienced notice condition 3 we mainly expected confirmation of their earlier choices. However, at this point we could study which of the practices in the short notices were considered harmful or unproblematic.

themselves. 14 participants had an age of under 20, 16 were aged between 20 and 25. They spent an average of 26 hours a week on their home computer (std. dev. of 12), and 2.5 hours a week on work computers (std. dev. of 4).

B. SURVEY RESULTS

The tables below describe the results of the two surveys we administered to each user. Table 1a describes the survey we gave to users before the task, which concentrated on user concerns. Table 1b describes the survey we gave to users after they performed the tasks, which concentrated on users capabilities. From the survey results in Table 1a, we saw that our users were mostly concerned with programs that gave pop-up advertising, sent personal information, or affected their systems performance (crashing, slowing down, etc). Our users seemed least concerned about monitoring behavior that the program would use to provide updates or assist in diagnostics of software problems. Finally, our users indicated that they were mildly concerned about monitoring their actions on their machines, such as web sites visited and programs installed.

In terms of their capabilities, our users represented more sophisticated computer users. While this was most likely the result of the sample we had (late teen, college undergraduates who spent on average 26 hours per week on their home machines). It was surprising how sophisticated they were since none of the sample were actually pursuing a technical degree. To some extent, they represented the growing sophistication of the average young computer user. Half of the users had changed the value of a registry key at least once, or could determine the amount of RAM an application was using as well as the amount of CPU time an application consumed. In the post-interviews we confirmed that they had indeed learned many of these techniques from more technical friends in an effort to combat spyware, and determine what could be affecting their machine's performance.

Questions	1 - not concerned	2 - minimally concerned	3 - moderately concerned	4 - very concerned	5 - extremely concerned	Mean	Median	Mode	STDDEV
This program collects the title and web address of the websites you visit.	10%	23%	29%	32%	6%	3.03	3	4	1.11
This program collects information about what software is [illegible] on your computer.	3%	23%	32%	29%	13%	3.26	3	3	1.06
This program collects your first name, city, ZIP code, country and time zone.	3%	3%	19%	29%	45%	4.10	4	5	1.04
This program collects information about how the program crashes and this information is reported to the company to prevent crashes from happening in the future.	55%	23%	16%	6%	0%	1.90	1	1	0.99
The information is collected whenever you use your web browser to build a profile of your browsing behavior.	6%	19%	35%	16%	23%	3.29	3	3	1.22
This information collected is used to show advertisements on your computer.	0%	10%	6%	29%	48%	4.06	4	5	1.12
This program keeps track of your computer memory usage and makes an automatic backup of your data if your computer is likely to crash.	32%	26%	29%	3%	10%	2.32	2	1	1.25
The information collected is used to create personal accounts, [illegible] to your identity.	35%	48%	10%	6%	0%	1.87	2	2	0.85
The information collected is used to create a profile linked to your identity.	0%	0%	16%	35%	48%	4.32	4	5	0.75
This program will cause your computer to shut down.	0%	3%	16%	19%	61%	4.36	5	5	0.96
This program will cause your computer to crash.	0%	0%	0%	3%	97%	4.97	5	5	0.18
This program will prompt you to install updates to the program when they are available.	39%	32%	26%	3%	0%	2.03	2	1	1.03
This program will automatically add other updates to your computer without asking for [illegible].	13%	19%	35%	23%	10%	2.97	3	3	1.17
This program can be un-installed using the add/remove programs feature that comes with Windows.	65%	6%	13%	10%	6%	1.87	1	1	1.34
This program can only be uninstalled manually.	35%	23%	16%	13%	13%	2.71	2	1	1.51

Table 1a: Survey Results of User Concerns

Questions	1 - I have done this many times	2 - I have done this at least once	3 - I have never done this but would be comfortable trying	4 - I'm not comfortable and would ask someone to help	5 - Not sure	Mean	Median	Mode	STDDEV
Changing the value of a registry key	43%	7%	3%	17%	30%	2.83	2.50	1.00	1.80
Changing keyboard [illegible]	35%	26%	10%	26%	3%	2.61	2.50	3.00	1.04
Configuring an anti-virus program	30%	13%	23%	33%	0%	2.60	3.00	4.00	1.25
Configuring a firewall program	30%	17%	17%	33%	3%	2.60	3.00	4.00	1.28
Reinstalling the operating system	40%	17%	13%	23%	7%	2.40	2.00	1.00	1.40
Configuring proxy settings on your internet browser	30%	13%	23%	33%	0%	2.60	3.00	4.00	1.25
Remove programs from your computer	50%	0%	0%	50%	0%	2.50	2.50	4.00	1.53
Watching what tasks are running on your computer	43%	3%	10%	37%	7%	2.83	3.00	4.00	1.43
Finding files on your computer using windows explorer	23%	17%	13%	43%	0%	2.70	3.00	4.00	1.34
Determining what programs are installed on your computer	33%	10%	10%	43%	3%	2.63	3.00	4.00	1.43
Changing attributes of files and folder	20%	17%	10%	37%	13%	2.97	3.50	4.00	1.50
Determining how much RAM your computer is using	10%	7%	37%	20%	26%	2.97	2.50	3.00	1.40
Determining how much processor time an application is using	30%	20%	27%	13%	10%	2.53	2.50	1.00	1.33

Table 1b: Survey Results of User Capabilities

C. INSTALLATION DECISIONS

1. WHAT FACTORS CONTRIBUTED TO PARTICIPANTS' DECISION TO INSTALL PROGRAMS?

One of the goals of our study was to observe user behavior installing programs in a near-natural setting. It allowed us to ask

questions about their motivations and actions. We observed whether users paid attention to EULAs, and if so, what particular information they obtained or sought. Other factors we examined are why participants installed programs, and what process they followed. We discovered that our participants shared general concerns about what is installed and the effect it has on their computer. Participants varied widely in their installation procedures.

2. INSTALL PROCESS

Participants' reasons for installing programs varied. Some participants only installed applications that they felt comfortable with. Other participants installed everything with the intention of checking out unknown programs and uninstalling them later. The following categories demonstrate some of the main strategies we observed (we note that we do not consider this to be an exhaustive list of all possible user motivations or to be representative of the general population):

- **Install first, ask questions later:** These participants generally installed all programs at once, with the intention of examining them in greater detail later. They tended to consider themselves computer savvy, with the ability to remove or configure programs after installation to avoid adverse affects to their machine. They felt sufficiently familiar with the installation process and tended to click through each screen very quickly.

- **Once Bitten, Twice Shy**: These participants were somewhat computer savvy, but they were influenced by past negative experiences. One participant had recently been a victim of a phishing attack, while another had a program "totally cripple" her laptop. They have had past computers crash or become inoperable because of rogue programs or viruses and often lost data These users tended to be overly cautious, and they chose to install applications only if they felt those applications were absolutely required. They typically skimmed EULAs and programs' information for key phrases such as "ads," "GAIN," or "popups" to avoid choices that would potentially be harmful.

- **Curious, feature-based**: These participants were primarily interested in potentially new and interesting features delivered by the selection of programs. They would only install an application if it was popular or offered something that they would want or need. These users would typically install a program such as WeatherScope because they thought it was "cool" and "useful".

- **Computer-Phobic:** These participants were generally wary of anything that had to do with installing programs or configuring a computer. They sought assistance from their friends or other experts when they had problems, and they would generally request help with any install. One participant mentioned that her father was a savvy computer user and "passed on paranoia" to her. They were generally very concerned with any warning that popped up, and were reluctant to install anything.

3. INSTALLATION CONCERNS

1. Our participants shared a range of common concerns about installing software that we gathered in our post-installation interview sessions. In the interviews, we asked open-ended questions about their concerns with each application. We categorized these, and listed them below in order of importance:

2. Functionality (>80%) – A large majority of participants who expressed some form of concern were primarily interested in the functionality of the application. By functionality, they mean convenience, lack of other alternatives, its "cool factor" (direct quote) and its purpose. Participants were most interested in programs that are "necessary," "helpful," or "convenient, easy to use" and would add some "aesthetics."

3. Popups (~60%) – Popup advertising was the second largest concern out of our participants, across all categories of users. Many users had strong reactions to them. "I hate them!" was a reaction echoed by several participants. Many were

extremely reluctant to install a program that had popup advertising or seemed like it would. One participant stopped an installation after she saw the word "GAIN," which reminded her of Gator, a company that had put advertising on her machine before.

4. Crashing their machine, computer performance (~30%) – Some participants were worried that programs would crash their machine, take up space, or cause their machine to be unstable. This was especially a concern with the 'Once Bitten, Twice Shy' participants.

5. Installing additional software (~15%) – Participants were concerned about software that installed additional programs. "I don't want a lot of junk on my computer" remarked one user. "Junk" was classified as additional programs that ran in the background, that changed homepages, slowed the machine, caused it to crash and/or served ads.

6. Monetary cost (~10%) – Some users were concerned that they may be eventually charged later for software they installed, even though they did not enter any credit card information.

7. Sends information (<5%) – Our participants never directly mentioned privacy concerns as a reason to not install a program, but several mentioned that they would be wary of programs that collected personal information because they thought it would lead to spam or more ads on their machine. They referred to personally identifiable information such as email addresses.

4. WHAT DID USERS INSTALL?

We were interested what effect notice had on users installing programs. As discussed above, we ran three notice conditions on 31 subjects. We observed their behavior and asked them questions about their actions. A breakdown of subjects is included in Table 2.

	Number of Subjects
Control (EULA Only)	10
Generic Microsoft + EULA	10
Short Notice + EULA	11
Total	31

Table 2: Breakdown of subjects by notice condition

Table 2 indicates that additional notice overall (in the form of the generic Microsoft warning or the short notice) had only a marginal impact on the total number of installations (by ~10%, n.s.).However, the post-interview process showed that participants felt better informed in the notice condition 3 (short notice). In the following we describe in more detail their reactions to notice condition 2 (generic Microsoft notice) and notice condition 3 (short notice).

	Installs by notice condition
Control (EULA only)	36 (72%)
Generic Microsoft + EULA	31 (62%)
Short Notice + EULA	35 (63%)

Table 3: Total Installs for per notice condition

Notice condition	Participants who remembered seeing an additional notice	Participants who remembered the content of the additional notice	Participants for whom the notice affected their decision to install
Generic	6 of 10	8 of 10	4 of 10
Short EULA	11 of 11	10 of 11	7 of 11
Total	17 of 21	18 of 21	11 of 21

Table 4: Number of participants that could remember additional notices

5. GENERIC MICROSOFT NOTICE + EULA

Table 4 reproduces the number of participants that could remember seeing the generic Microsoft notice (60%), that could remember some content of the notice (80% with additional probing) and remember that it had some effect on their decision to install (40%). Some participants found the generic notices to be useful; particularly if the generic warning indicated to users that there was no known publisher. One participant stated "Edonkey didn't look good. The notice said 'unknown publisher', so I chose not to install it." However, none of the participants clicked on the link that provided more information about the publisher if the publisher's identity was known. Several users instinctively clicked through the notices without even reading them. When asked if they saw them, they said no, but when prompted with a blurred version of the notice they said, for example, that they have seen similar notices in the past. One participant mentioned that "it asked you whether or not you wanted to download it, [and] gave the company name, info and licensing agent."

6. SHORT NOTICE + EULA

Table 4 shows that all participants could remember having seen the short notice, and that 91% could remember some details of their content. 64% stated that the short notice influenced their decision to install the programs. Participants were generally enthusiastic about the short notices we created. One user wanted to know where we got it,

because he wanted to use it at home. Others remarked that they "were amazing," and that they would "love to see this, it would be really awesome!" When further prompted for reasons to use this kind of short notices, this participant remarked "I personally wonder how many people just install stuff [without thinking], wouldn't be surprised if it was the majority." Others stated that they used the information in the short notices to compare programs and assist their decision. One user said "the pop-up windows said the programs were no good, [and I] might not have known without them."

Most participants were able to recall parts of the content of the short notices as well. They mostly recalled the issues that they were most concerned about (e.g., pop-ups and system performance). Several users were concerned about information transfers to third-parties, and some mentioned that the information in the short notices "surprised them."

Despite the positive reactions, some users simply ignored them as well. Despite stating in the post-interview that they would like "clear and concise" information, they made comments such as, "It is hard to say if I would read them [short EULAs] even if you flashed IMPORTANT at the top. After the third or fourth one I wouldn't read and it would be easy to skip."

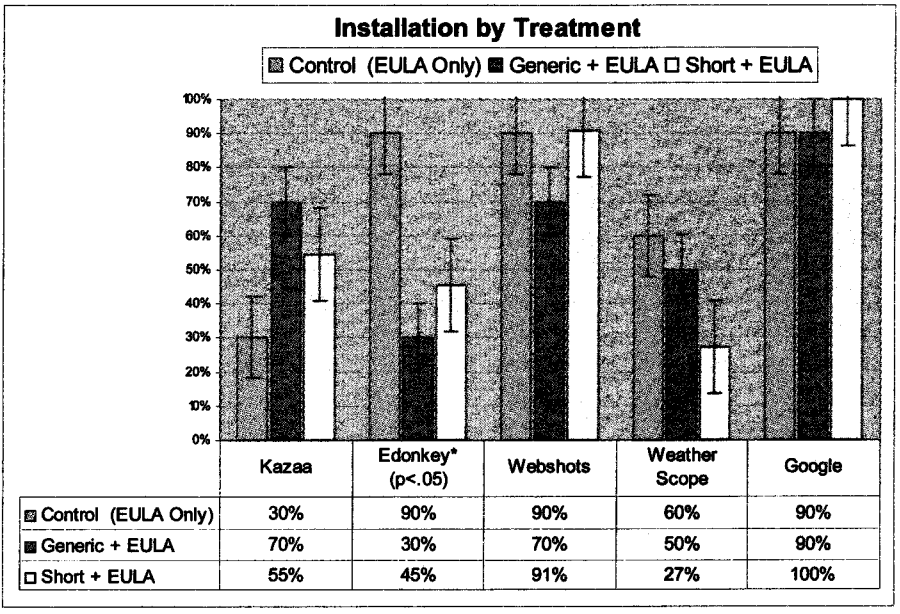
7. WHAT PROGRAMS WERE INSTALLED MOST?

For each notice condition we were also interested in what programs users installed. We saw that the Google Toolbar was the most often installed among all sets, whereas Weatherscope ranked last. Main reasons for this effect were brand recognition and prior experience. Users mentioned, for example, that Google "was a trusted brand name" and that they "thought Google toolbar did a good job at blocking popups."

While overall the difference in installations between notice conditions was not statistically significant, there was a significant difference in installations for Edonkey. Users remarked that Edonkey was generally unfamiliar, so any additional notice "spooked" them. In addition, as we will discuss in more detail later, in the case where users had notices they used these in some cases to compare between the two file sharing applications.

Weatherscope was rarely installed because it reminded users of a similar program called "Weatherbug," which was universally disliked because "it had too many popups" and it "crashed my machine." Users also mentioned that the benefits that are associated with programs such as Weatherscope or Weatherbug did not outweigh the higher cost of

dealing with popup advertisements. A user remarked "you can go to weather.com if you really want to check the weather, and then you don't have to deal with any popups."



	Kazaa	Edonkey* (p<.05)	Webshots	Weather Scope	Google
Control (EULA Only)	30%	90%	90%	60%	90%
Generic + EULA	70%	30%	70%	50%	90%
Short + EULA	55%	45%	91%	27%	100%

Figure 5: Graph of Installation by Treatment

D. NOTICE TREATMENTS

1. DID USERS LOOK AT EULAS?

Participants generally ignored EULAs. The *install first* users were especially adept at clicking through installation screens extremely quickly. Some users went through this process so quickly that they did not even remember clicking through the short notices and the Microsoft warnings as they popped up. One *install-first* participant remarked that "[t]he process is so standard, there is nothing to influence [your decision] to install or not. I just use all the default options and configure it later if I am going to keep it."

2. NOTICING NOTICE

We categorized whether users had read a notice as *not at all*, *skimmed* and *carefully*. *Not at all* meant that they did not glance at the notice and promptly continued to the next screen. *Skimmed* means that they may have passed their mouse over the EULA looking for keywords, or used the scrollbar to quickly browse through the contents. *Carefully* means that they actually read some sentences or a paragraph, before continuing on. We should note that in no case did the users attempt to read through all of the EULAs or even one EULA completely. In the case of the Generic Notices, because there was no scrolling involved, we only noted if they had read it at all. Cases were labeled as N/A if they were not relative to the installation. For example, if users quit before they were able to see any notice, or decided that they didn't want to install a program, or the program did not contain that feature, they were all marked as N/A and was not included in the computation.

Program	Totals Average	Control (EULA only)	EULA + Generic Notice	EULA + Short Notice
Read EULA				
Skimmed	37.89%	38.10%	50.00%	25.58%
Carefully	10.03%	7.14%	6.67%	16.28%
Not At All	52.08%	54.76%	43.33%	58.14%
Read Short EULA				
Skimmed	17.07%			17.07%
Carefully	60.98%			60.98%
Not At All	21.95%			21.95%
Read Generic Notice				
Read	41.03%		41.03%	
Not At All	58.97%		58.97%	

Table 5

Table 5 shows that the Short Notices were skimmed or carefully looked at almost 80% of the time, whereas the standard EULA and Generic notice were looked at on average of less than 50% of the time.

3. WHEN DID USERS STOP AN INSTALLATION?

In addition to data on whether users had read or skimmed an article, for 28 of the 31 users we had observational data about their actions during the installation process. This data was gathered by observing the installation process, and marking when users decided to stop an installation. From the graph in Figure 6 and the data in Table 6, it is apparent that the majority of the users in all treatments would complete an installation after they had started it. The most common case for not installing an application was either skipping it entirely or just opening it briefly before exiting (~15%). Once a user had decided to install an application, it was very rare that they would stop. Less than 6% total stopped installation at the EULA. In the treatments with the short or generic notices, users aborted an installation only 10% of the time.

Installation Process for 28 of the 31 users	Control (EULA only)	EULA + Generic Notice	EULA + Short Notice	Total
Didn't Open and Ignored	8.00%	2.50%	10.00%	7.14%
Opened Briefly then Stopped	8.00%	7.50%	4.00%	6.43%
Stopped Before the EULA	0.00%	2.50%	2.00%	1.43%
Stopped at the EULA	8.00%	2.50%	6.00%	5.71%
Stopped at Short Notice	N/A	N/A	10.00%	N/A
Stopped at Generic Notice	N/A	10.00%	N/A	N/A
Stopped after EULA	6.00%	0.00%	0.00%	2.14%
Completed Install	70.00%	75.00%	68.00%	70.71%
Total	100.00%	100.00%	100.00%	

Table 6

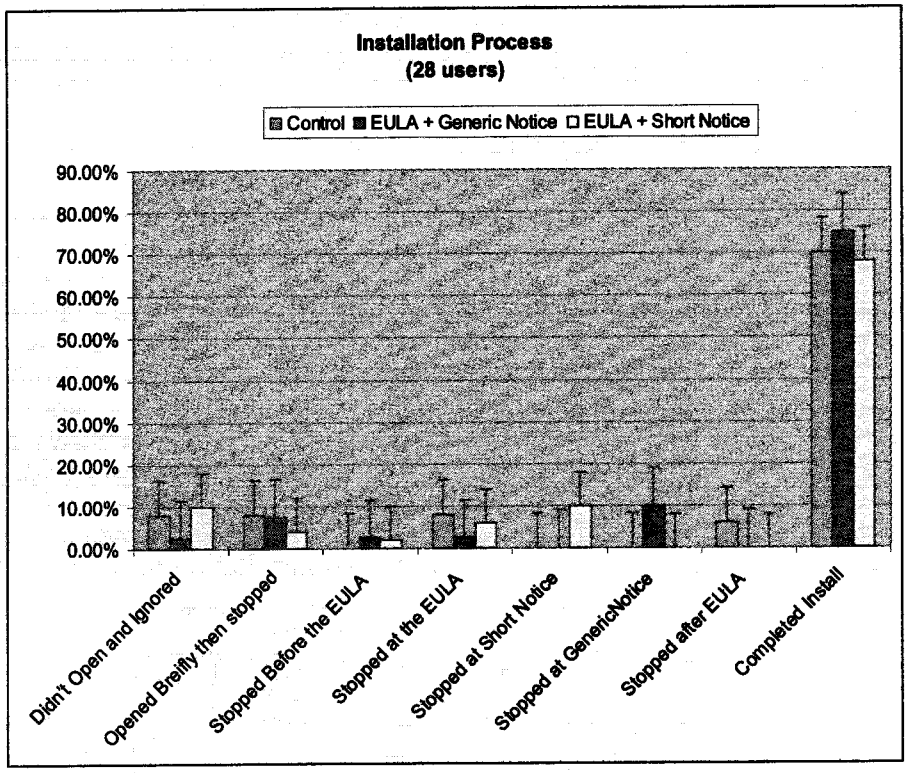


Figure 6

4. FILESHARING AS A "MUST-HAVE" APPLICATION

We discovered that among our user population and demographic, filesharing was a "must-have" application. Although users typically installed only one filesharing application, 23 of the 31 users felt that they should have at least one filesharing application. Users mentioned that filesharing applications were "very useful" and something that "everyone should have." However, in choosing the filesharing application to install, users frequently tried to determine which application would be less intrusive on their machine. Some users used the short notices to compare filesharing applications, while others were influenced by the fact that one was "trusted" (as indicated in the generic Microsoft warnings for KaZaA) and the other was "unknown" (and therefore less trustworthy). Overall, more users installed eDonkey over KaZaA. The primary reason for this decision was a negative experience with KaZaA. For example one user complained that "it

crashed my machine," "I had to reinstall everything again," and that "it had too many popups."

Notice condition	Didn't install one Filesharing program
Control (EULA Only)	1
Generic + EULA	2
Short notice + EULA	4
Total	7

Table 7: Users who didn't install a Filesharing Application

5. VAGUE SHORT NOTICES CAN CREATE A FALSE SENSE OF SECURITY

An interesting find was the higher number of installations for KaZaA in the short notice treatment as compared to the control. During the post-study interview participants indicated that KaZaA "didn't seem as bad" as Edonkey. The number of users preferring KaZaA over Edonkey was especially pronounced in the short notice treatment. As discussed above, users typically wanted to install one or the other, and used the short notices to compare the programs. Edonkey disclosed more about the software's functionality, and gave users the option to opt-out of certain features, and KaZaA did not. The short notices that were constructed based on each programs disclosure reflected this difference. Our short notice treatment reflected the relative complexity of the two programs. Despite the fact that the Edonkey EULA was more friendly to users—disclosing more about program functionality and providing users with opportunities to reject certain features—the greater complexity was evident in the short notice and was viewed by users as unfavorable. Below we list the contents of the eDonkey short notice and the KaZaA short notice. From the two short notices below, we can see that eDonkey discloses more information about what personal information is being collected, but that the users have the ability to opt out of this process. KaZaA says less about the type of information being collected and does not offer an opt out. In this case, providing vague information, which led us to create a simpler short notice, created an impression of increased security or at least less risk

6. KAZAA AND EDONKEY SHORT NOTICES

Below we list the actual short notices used to describe each program.

How the eDonkey Agreement Affects You and Your Computer

What information is collected?

- Personally identifiable information like your name.
- Information about your browser, computer operating system and Internet Service Provider.
- The title and web address of the websites you visit.
- Information you enter into forms on websites and what you clicked on.

How is this information collected?

- Information is collected whenever you use your web browser (Internet Explorer), whether or not you are using eDonkey.

How is this information used?

- The information collected is sent to third parties.
- The information collected is used to display pop-up advertising on your computer.
- The information collected is used to create general statistics about all users of the system.

How does this installation affect your computer?

- You are installing four programs. Every time you install a new program it has the potential to slow down your computer, slow down your web browsing, and/or cause other programs to crash.

- This program will show popup advertising on your machine when you browse the web.
- This program will automatically add new programs to your computer without asking you.
- This program will install a new toolbar in your web browser, and change your browser start page.

How KaZaA Agreement Affects You and Your Computer
What information is collected?

- The title and web address of the websites you visit.

How is this information collected?

- Information is collected whenever you use your web browser (Internet Explorer) whether or not you are using KaZaA.

How is this information used?

- The information collected is sent to third parties.
- The information collected is used to display pop-up advertising on your computer.
- The information collected is used to create general statistics about all users of the system.

How does this installation affect your computer?

- You are installing four programs. Every time you install a new program it has the potential to slow down your computer, slow down your web browsing, and/or cause other programs to crash.
- This program will show popup advertising when you browse the web, whether or not you are using KaZaA at that time.

- This program will automatically add new programs to your computer without asking you.

- This program will install a new toolbar in your web browser, and change your browser start page.

7. EULAs AND TOS AS LEGALLY BINDING DOCUMENTS

Our participants were generally ambivalent towards the EULAs and ToS in the software they installed. Table 8 shows that while almost all participants were aware that they were agreeing to a set of terms by installing the software (30 of 31), they were generally unable to recall the content of the agreement (only 8 of 31 recalled the content), and it rarely influenced their decision to install a program (only 6 of 31 mentioned that it influenced them). The participants who did recall contents of the EULA remarked that it was generally about information that referred to the software product itself, such as "copyright notices," "company policies," or "reverse engineering the product or using it for unintended purposes." Almost none of the participants, including the more computer savvy "[i]nstall first, ask questions later" users, had any idea that the content of the EULAs and ToS actually discussed applications that would be installed, data that would be collected, and companies that would access their data. There seems to be a disconnect between user expectations of EULA content and actual EULA content. One user summed up this confusion by stating "They should have notices to show what they are really installing on the computer. They trick you [into] thinking it is just a license agreement, [you] hit OK, and then you get an advertising bar or a lot of junk!"

Notice condition	Participants aware that the Software EULA was a contract	Participants who had an idea of what the agreement contained	Participants for whom the EULA affected their decision to install
Control (EULA only)	10 of 10	2 of 10	3 of 10
Generic + EULA	10 of 10	5 of 10	2 of 10
Short + EULA	10 of 11	1 of 11	1 of 11
Total	30 of 31	8 of 31	6 of 31

Table 8: Understanding EULAs as Contracts

E. Regretting Installation Decisions

We were interested to learn whether accurate information about software behavior would lead users to change their mind about program installations. We showed the short notices to all users at the end of the survey to determine whether users read them earlier (this applies to the short notice condition only) and if they thought they would have influenced their installation decisions (applies to all notice conditions). Users were asked to read each of the short notices carefully, and to decide whether they would like to reverse their earlier decision to install or not to install. This approach allowed us to gauge whether individuals regretted their installation decision. Regret or disappointment materializes if an earlier decision appears to be flawed in retrospect, and/or when the obtained result does not match prior expectations [17].

We were interested in examining the relationship between users reading or skimming a Short Notice, EULA or Generic warning and regret and installation decisions. We broke down possible types of regret into these categories:

1. Users regretted their decision and would uninstall the program.

2. Users regretted their decisions and would install the program.

3. Users did not regret their decision and would keep the program installed.

4. Users did not regret their decisions and would keep the program uninstalled.

While it is helpful to look at regret in these terms, we were interested in the effect of notice alone, and in coordination with other factors, on regret. Therefore we decided to look at the following additional factors:

1. Previous Experience – Users were asked if they had previously heard of an application, and if so, whether this had influenced their choice to install the program.

2. Reading a notice – During the installation process, the observer recorded whether users had looked at a notice or not.

3. Influence of a notice – After the installation process, users were asked if the notice influenced their decision or not.

4. Stopping an installation – During the installation process, the observer noted at what point a user would stop installing a given application.

5. Reasons for installing/not installing – Users were asked after completing the installation, their reasons for installing or not installing a given program.

Overall, we found that regret was highest with Weatherscope and the filesharing programs. Users were generally happier with their decision to not install these programs after reading our short EULAs. Popups, performance issues, and the potential disclosure of private information to third parties all contributed to user regret. Some users were upset, stating "I didn't install that!," while others were surprised at the extent of information collection they had agreed to by installing and using certain programs. Some users remarked that they would remove programs that had popups. They stated, "if I had known this had popups I wouldn't have installed it."

1. REGRET WITH FILESHARING APPLICATIONS

Despite the regret that some users felt for filesharing programs, many indicated that they would still install them. One user who expressed regret at her decision to install eDonkey said "if all free music programs do this, and I can't find anything better then I'm going to install it. For a free photo program it might not be worth it, but for free music it is." Another user added "I really don't like that it adds other software, but I would still keep it because filesharing is worth it."

2. REGRET WITH TRUSTED SOURCES

In the case of Google Toolbar, the program with the greatest brand recognition among our users, the reasons for uninstalling were related to performance and space issues, rather than concerns with privacy or computer security issues. One user indicated that he "didn't want another thing in [his] browser window" and that [he] liked to keep the minimum amount of programs running at any given time.

3. REGRET ACROSS NOTICE CONDITIONS

We studied the degree of participant regret over an installation decision in relation to each notice condition. We expected that users would experience less regret when they were better informed (i.e., being presented a short notice or a generic Microsoft notice in addition to the EULA). In fact, participants verbally indicated that especially the short notices had a substantial effect on their decision to install or not. Compared to the control notice condition, participants experienced regret about 15% less often when presented with either a short notice or a generic Microsoft warning. Given the size of the study, this effect is not statistically significant; however, we believe it merits future consideration.

The set of programs in our study included two applications that the community of our participants had experienced high regret and low regret with. We determined that there were some applications that had a high install rate, low regret rate and were generally positively commented upon (e.g., Google). Conversely, there were some applications that were installed less frequently, had a higher level of regret, and were viewed negatively. The applications with low regret were Google and Webshots, and those with higher regret were Edonkey and Weatherscope. We divided the applications into two groups, and examined user regret across each notice condition. Table

9 shows the percent of programs that users regretted versus those that they would keep. The total number of programs removed was the net of programs that users regretted installing and programs the user regretted not installing. This number was then subtracted from the total number of installs, and normalized across all programs and treatments. From the graph in Figure 7, we can see that regret was generally highest in the EULA treatment, and lower and about the same for the generic notice and short notice treatment.

Google toolbar was the highest trusted application, with 93% of users installing it, and 83% of the people deciding to keep it after reading the short notice in the post-study interview. Weatherscope was on the other end of the spectrum, with just 47% of the recipients choosing to install it overall, and none of the thirty-one users choosing to keep it.

Figure 7 gives a detailed breakdown of each program installed, and illustrates the balance between programs that our users decided to keep, and those they decided to remove. The top half of each bar represents the percentage of users who chose to remove the program while the bottom half of each bar represents the number of users who decided to keep it after being asked to read through each short description. Solid colors indicate that all users either kept or removed the program. By looking at Figure 7, one can see that users decisions to install were generally consistent within each program group across all treatments. For example, we can see that in the case of Google, roughly 90% of all users across treatments chose to keep the toolbar, where as in Weatherscope all users chose to remove it.

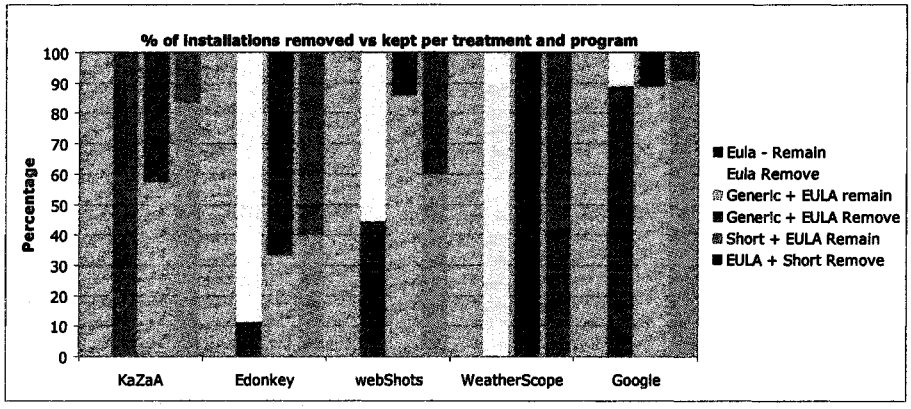


Figure 7: Programs Removed v. Programs Kept

	Regretted installing	Regretted not installing
Control	19 (52%)	2
Short notice	13 (37%)	2
Generic notice	11 (35%)	0

Table 9: Installation Regret per Notice condition (Number of installations regretted)

We found (see table 10) that users in the two notice conditions had lower levels of regret compared to the control condition. Results between these notice conditions were not statistically significant, but supported by participant comments in the post-study interview.

	Low Regret Applications	High Regret Applications
Control	6	13
Short notice	6	5
Generic notice	1	9

Table 10: Regret for "low regret" versus "high regret" applications

We also studied whether the different notice conditions influenced users by preventing them from installing applications that were deemed "high regret" by the community.

Table 11 shows that the number of "high regret" installs is similar for both the short and generic notices and 6-7 programs less compared to the control case. Participants also installed more programs that the community considered "low regret" in the short notice case, but fewer programs in the generic case. This may be due to the "warning" rather than "informing" character of the generic Microsoft notice that may have scared participants away.

	Installed "useful"	Installed "not useful"
Control	18	15
Short notice	21	8
Generic notice	16	9

Table 11: Installation of "useful" versus "not useful" applications

F. PRIOR KNOWLEDGE, READING NOTICE AND REGRET

The results from measuring regret seemed to suggest that the additional warnings may have had some effect on user behavior. Although for the small number of participants we had per treatment, there was no statistical significance between treatments for regret. The data and post study interviews seemed to suggest that for users who did read the shorter notices, they may have had some effect in matching or reaffirming their preferences, thereby decreasing instances of regret. This seemed contrary to what we had observed. As shown in the tables on installation behavior, users generally ignored all notices and seemed unlikely to stop an installation once they had started it. The number of regret cases we observed was too small to perform statistical analysis on beyond simple descriptive statistics. However, we decided to look more closely at anecdotal evidence of how regret, prior experience, and reading notices and user comments were related to help motivate further studies.

Table 12 below summarizes regret by users who had indicated they had prior experience with an application or not. In cases where users had prior experience with a program, one would expect regret to be lower. Because we chose programs that were popular, it is conceivable that users had already formed opinions about an application before they installed it.

In Table 12 we see that overall, users who had prior experience with a program did seem to have lower regret (13% and 23% compared to 50% for the control). In addition, they seemed to have lower regret in each group as well (13% compared to 25% for the generic notices, and 23% compared to 50% for the short notices).

The next column shows the number of users who expressed regret who were also either influenced or not influenced by the notice. The next columns show how many of those users regretted their

installation per program. By comparing the grey bands with the bands below it, we can see that regret for those unfamiliar with an application seems to be higher than those who claim they were influenced by prior knowledge of the application. It is interesting to note though, that in all cases the incidence of regret for the notice treatments is still less than the control.

	Total incidences of regret	# of users	Of these users, the # of times that they expressed regret per program				
			Edonkey	Google Toolbar	KaZaA	WeatherScope	WebShots
Control (Baseline)	24 of 50 -50%	10	8 of 10 -80%	1 of 10 -10%	4 of 10 -40%	6 of 10 -60%	5 of 10 -50%
Generic	10 of 45 -22%	9	2 of 9 -22%	0 0%	3 of 9 -33%	5 of 9 -55%	0 0%
Influenced by prior experience	2 of 15 -13%	3 of 9 (~33%)	0 0%	0 0%	1 of 3 -33%	1 of 3 -33%	0 0%
Not influenced by prior experience	8 of 30 -26%	6 of 9 (~67%)	2 of 6 -33%	0 0%	2 of 6 -33%	4 of 6 -66%	0 0%
Short Notice	16 of 50 -32%	10	5 of 10 -50%	2 of 10 -20%	2 of 10 -20%	3 of 10 -30%	4 of 10 -40%
Influenced by prior experience	7 of 30 -23%	6 of 10 -60%	3 of 6 -50%	1 of 6 -16%	0 0%	0 0%	3 of 6 -50%
Not influenced by prior experience	9 of 20 -50%	4 of 10 -40%	2 of 4 -50%	1 of 4 -25%	2 of 4 -50%	3 of 4 -75%	1 of 4 -25%

Table 12

Below we will quickly summarize some of the additional anecdotal findings from our data.

1. READING NOTICE AND REGRET

We found that participants, who looked at short notices, generally had less regret than those who did not, although not by a large margin. We noted a similar result with the generic notice treatment.

2. INFLUENCE OF PRIOR KNOWLEDGE AND SHORT NOTICE ON REGRET

We found that users who indicated that they were influenced by both prior knowledge and the short notice were less likely to experience regret. In addition, we found that this was the case for programs that were both installed and not installed. For example, in the case of KaZaA, six users in the short notice condition claimed to have heard of KaZaA, and five of them mentioned being influenced by their previous experience. In addition, they mentioned that the short notice influenced their decision as well. It is interesting to note that of the users who did not change their mind in this case (5 out of 6), they

were almost evenly split between those who installed KaZaA and those who did not (three installed, two did not). This implies that in some cases, the short notice is useful in affirming users' belief or experience of a given product. Looking back at these users responses, we discovered that they found the short notices useful, even though their offer merely confirmed what the users claimed they already knew.

F. ANALYZING TRADEOFFS

In our study, users were asked to evaluate the P2P filesharing programs: KaZaA and Edonkey. P2P programs were largely considered a "must have" application by our user population. Generally, every user installed at least one, but rarely installed both. This leads us to wonder what factors influenced the choice between the two programs. Installations of these programs across all treatments were roughly split in half (~50% installed KaZaA, ~60% installed Edonkey). We found that users considered their previous experience with a program(s), referrals from 'experts' they know, and/or other means of comparison. We summarize these findings below.

1. PREVIOUS EXPERIENCE

Our users were more familiar with KaZaA than Edonkey. 92% had heard of KaZaA. 82% mentioned that they had prior knowledge or experience with KaZaA, which contributed to their decision to install it or not. Only 18% mentioned that they had heard of Edonkey, with only 11% saying this factor had an effect on their decision to install. Users familiar with KaZaA, ranged from people who found it "useful to get what I want" to those who had negative associations, "I had it and it crashed my computer. I had to reinstall everything," and also "I had too many popups." In the case of Edonkey, users who were familiar with it commented more on functionality, stating "I can find what I want." It was interesting to note that if negative reactions alone accounted for users' decisions to install KaZaA, then the installation would be less than the 50% we observed. In eight cases, users decided to either not even open KaZaA, or terminated the installation immediately after opening the program, as opposed to zero cases in Edonkey. Users seemed to be employing some criteria, in addition to prior experience, so we examined the nature of these comparisons.

2. COMPARISON

Users generally relied on several factors to compare programs, including the short and generic notices. In the control group, 9 out of 10 users chose Edonkey, while only 2 of 10 chose KaZaA. In the additional notice cases (short and generic), installation of Edonkey dropped to roughly the same as KaZaA (4 to 6 installs in the Generic case, and 6 to 5 installs in the Short Notice case). In the case of Edonkey, with which our user base was less familiar, users exhibited more initial caution in installing this program, and relied more heavily on other cues during the install process. One user noted, "I didn't know what it was, I saw the unknown program warning and decided that I wouldn't install it." 3 of the 8 users in the Generic warning treatment stopped their installation after seeing the generic warning popup, as opposed to 0 in KaZaA, a more familiar program. In the short notice case, equal numbers of users stopped at the short notice. In post-study questions about installation decisions, we found that users tried to use the short notices to compare the features and trade-offs of the two programs. One common feature among the two programs was "popups" and some users mentioned "spyware" in the post-study interview. Some users would choose the program that they felt was more useful, and rely on tools like Google Toolbar to block popups that the program would provide. "[Popups] are a necessary evil, but I got [Google Toolbar] to block them so they won't be annoying." We found that users also used the short notices during the post study interview to compare programs when they were asked whether they regretted installing the program or not. We found that users would use short notices to measure tradeoffs between the two programs, and sometimes reverse their decisions about which program to install.

3. COMMON DISCLOSURE PROBLEM

The KaZaA EULA was more vague than the Edonkey EULA. Consequently the KaZaA short notice tended to be more vague than the Edonkey short notice. We found that when users compared the programs as presented in the short notices, they often tried to choose the software that would limit their exposure to third party software and advertisements, while providing the desired functionality. The inconsistency between disclosures in the KaZaA and Edonkey notices was magnified by the short notice treatment. This led to a perverse

result, where users seeking to limit spyware-like behavior ended up choosing the more invasive program. Providing a common means of describing the add-ons and attributes each program installs would assist users in their comparisons, and help them to make choices more closely aligned with their values. This suggests that in the absence of a common set of disclosures, short notices could have the unfortunate effect of subverting users efforts to limit their acquisition of spyware.

Program	Hyperlinks	Locations	Opt-Out	Opt-In
Edonkey	2	15	6	1
Google Toolbar	2	9	1	0
KaZaA	4	78	5	0
WeatherScope	0	23	0	0
WebShots	0	6	1	0

Table 13

VI. COGNITIVE WALKTHROUGH OF CURRENT EULA DESIGN

A. WHY ISN'T THE EULA SUFFICIENT?

While our experiment shows that additional research on the utility of short notices is warranted, EULAs in their current form do little to inform users about software functionality. As described above, EULAs are frequently the only method used to inform users about program functionality. In addition, EULAs are rarely examined or acknowledged by users during the installation process. Because they performed so poorly, we decided to use a technique in HCI known as a cognitive walkthrough to explore the benefits and shortcomings of current EULA design. While almost all software products have some form of EULA or TOS, they are by no means all equal in content, presentation, and deployment. Below we analyze the EULAs presented with the software used in our study.

B. THE PROBLEMS WITH EULAS

EULAs serve a dual purpose of providing users with information regarding their choices as well as providing software vendors

protection from legal liability. Given their perceived role in contract formation, it is important for practitioners, policy-makers, and courts to understand the limits of EULAs as a tool for conveying information to consumers. Regulating agencies have not created a set of guidelines for software EULAs. There is a general perception that EULAs are ineffective at least in part because consumers don't read them. Anecdotal evidence supports this impression. For example, one software provider included a $1000 cash prize offer in the EULA that was displayed during each software installation, it took 4 months and 3,000 downloads of the software for someone to notice the clause and claim the prize [17].

1. ANATOMY OF A EULA

Based on previous work and anecdotal evidence, we believed that EULAs are ineffective in communicating information to users by design. To explore this hypothesis, we decided to categorize and analyze the current methods software vendors employ in EULAs to inform users. We research aspects of the design that contribute to their ineffectiveness.

We looked at the software EULAs in the five programs used in our study, and focused on features—such as font size, readability, length and time to read—considered important in the regulatory efforts examining notices discussed above. We looked at additional factors such as the number of screens devoted to the EULA during installation, the method of presenting the EULA (scroll box, drop down, outside link), and options for controlling third party software or internal features that displayed advertisements, transmitted user information or modified existing settings (such as the homepage). We were interested in how users interacted with the EULAs, as well as how frequently they noticed or used the various strategies for controlling their desktop experience.

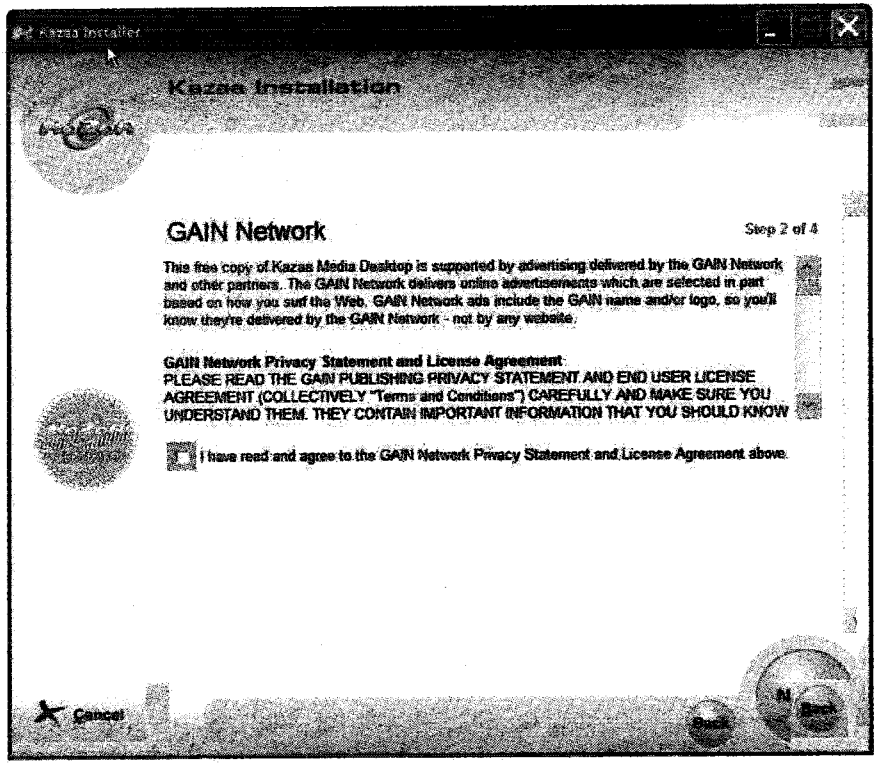
2. EULAS AND TOS APPEARANCE

Our participants found EULAs unhelpful. They stated that the "font was too small," they were "too long," and "full of legal mumbo-jumbo." A few users had read parts of EULAs carefully on one occasion, but eventually gave up on reading them because they were long and confusing. Our participants had several suggestions about how EULA presentations can be improved. Most notably they wanted EULAs to be "shorter, easier to read, and in very accessible language." One participant stated that she would like to see something "that

would tell you exactly what you want to know. [It would] provide a summary first, bold whatever is important, bold what is in the software, who is using it, and say if it is safe to download."

A. CURRENT EULA DESIGN

In analyzing the five EULAs, we documented common strategies for gathering consent and informing users in the program during installation. (We believe these are representative of strategies broadly employed across the software industry.) In the table below [Table 16], we list the strategies as well as their frequency of occurrence for each program [Tables 13]. These strategies are described below:



- Scroll Box containing EULA text – Users are provided the text of the EULA agreement in a scroll box.

- Force a choice to move to the next screen – This choice can be implied (users are connecting to a decision by clicking next) or strict (Users cannot proceed to the next screen before they make a choice about some feature or click some confirmation screen).

- Hyperlinks to outside sites and policies – Users are provided clickable links to additional EULAs and policies pertaining to the program (i.e., privacy policies, terms of service, etc.)

- Locations of third parties and policies – Users are provided information about the location of additional information pertaining to the program, such as laws, arbitration rules, but are not able to access it by via a hyperlink.

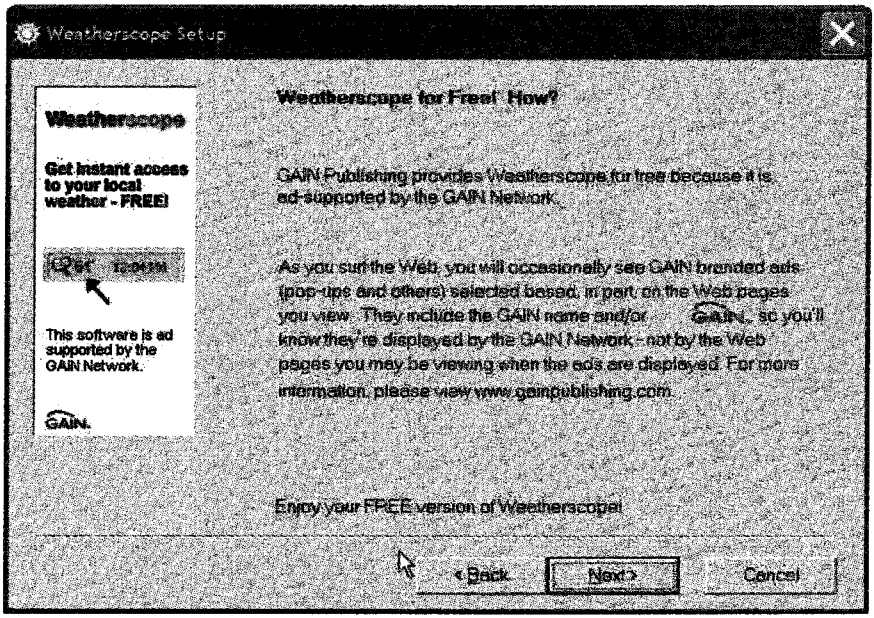


Figure 8: Example of a program describing advertising it installs

- Opt-out options- Users are provided checkboxes or radio buttons as a means to opt-out of features that

modify existing settings (home page), transmit user information or add-ons from third part vendors that send information or provide advertisements.

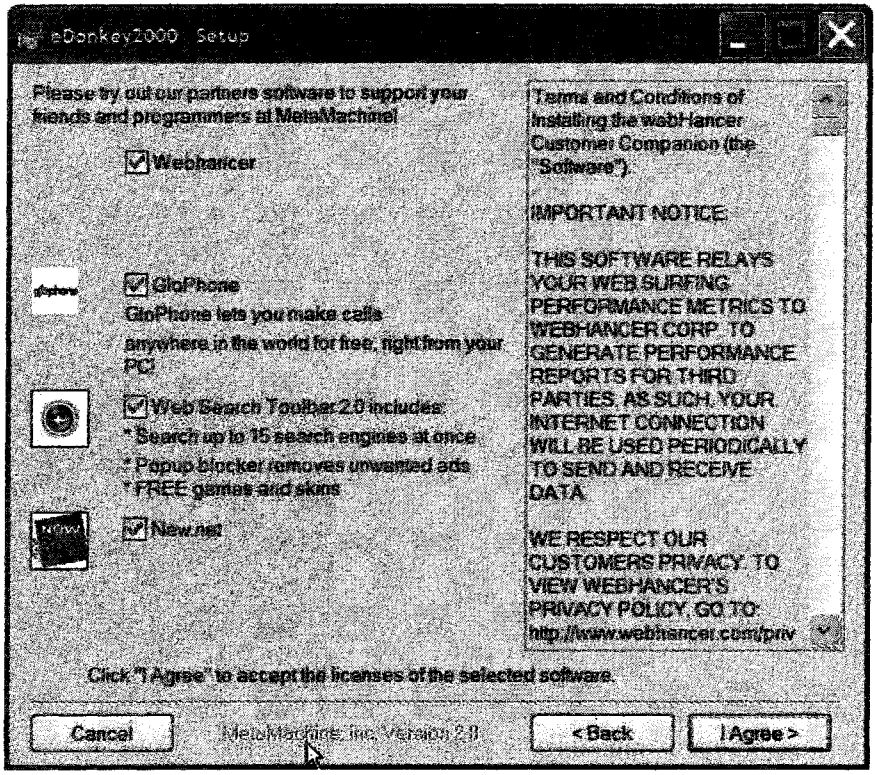


Figure 9: Example of a notice using opt-out

- Opt-In option – Users are provided checkboxes or radio buttons as a means to opt-in of features that modify existing settings (home page), transmit user information or add-ons from third part vendors that send information or provide advertisements.

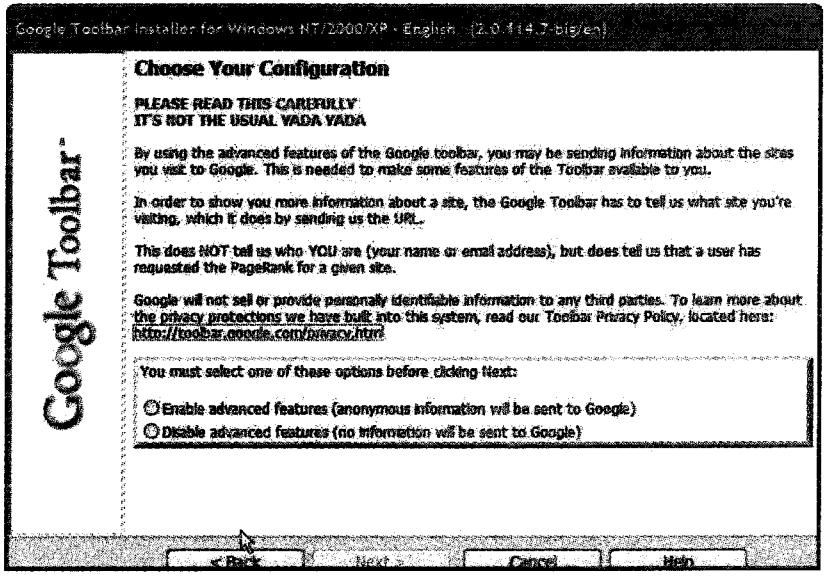


Figure 10: Example of a notice using opt-in

Program	Total EULA words in program	Total EULA words in first order links	Total EULA words	Estimated time to read[17] in minutes
Edonkey	2745	919	3664	30.53
Google ToolBar	1922	504	2426	20.21
KaZaA	17458	193	17651	147.1
WeatherScope	2856	N/A	2856	23.8
WebShots	1374	N/A	1374	11.45

Table 14

[17] Based on 120 efficient words per minute (ewpm) for the average reader.

Because the text box EULA was a common means of providing information, we examined them in more detail. We compiled a word count of each EULA, calculated the average words per screen, and estimated the time it required to read them [Table 14]. In our test, no user read an entire EULA, or even substantial portions of it. At best, they would scan for keywords, or try to find key sections that were interesting. Links to external sites were only clicked five times, (5%). When available, users availed themselves of the opt-out option over half of the time (52.7%). The option was only available for 3/5 of the applications we looked at.

Program	Hyperlinks	Locations	Opt-Out	Opt-In	Opt-out of any choices	Go to any external links
Edonkey	2	15	6	1	46.40%	0%
Google Toolbar	2	9	1	0	60.70%	3.60%
KaZaA	4	78	0	0	N/A	14%
WeatherScope	0	23	0	0	N/A	N/A
WebShots	0	6	1	0	50%	N/A
Total	8	131	8	1	52.37%	5.87%

Table 15

Program	Total Screen Count	Install Screens Dedicated to EULAs	Forced Choice Implicit	Forced Choice Strict	Scroll Box EULA
Edonkey	7	2	3	2	2
Google Toolbar	3	2	3	1	1
KaZaA	4	2	3	2	2
Weather-Scope	4	1	1	1	1
WebShots	4	1	2	0	1

Table 16

We also used common readability statistics to estimate the overall range of readability of the EULAs. We used the Flesh-Kindkaid reading level test in Microsoft word. Flesch Reading ease is a measure from 0-100, with a higher score indicating easier reading. We found that the EULAs analyzed had Reading Ease measures under 40. All EULAs Flesch-Kincaid Grade Level were grade 12.

3. EULA DESIGN IMPRESSIONS

While we were not able to keep track of the exact time it took users to install each and every application during the course of our study, we were able to get a general sense of how long users took to complete each installation task. In some cases, users completed all of the installation screens in less than 15-20 seconds, spending less than a couple of seconds per screen.

In no case did a user take more than 2-3 minutes to install an application. Users were typically able to complete all installations in less than 15-20 minutes including the programs actual installation time. This time span is obviously insufficient for users to read, let alone comprehend, the EULAs. Indeed, the entire time it took users to examine, install, and configure all five applications is less than the time it would take to read any single EULA presented.

In addition to reading times, users confirmed that the text was written at a level that thwarted their use and understanding. Compounding this problem, we documented a profound disconnect between what users expected EULAs to contain and what they contained in fact. While users recognized that there was some form of agreement, they had widely different, and generally inaccurate, impressions about the EULA contents. This mirrors results in earlier surveys on web privacy. It is important to note that users were not being lazy or careless, rather they simply believed that the majority of the information in a EULA did not pertain to them, was too generic, or standard "legal mumbo-jumbo."

We join others in concluding that EULAs are ill suited for the task of conveying information to consumers and obtaining consent. There is little in the design of EULAs that would suggest they are useful for informing and educating users. While this is not altogether surprising for HCI practitioners, EULAs are currently considered the state of the art in notice and consent, and are routinely enforced by courts. Fixing EULA design is an important activity with broad implications.

VII. CONCLUSIONS

We have conducted a user study in a controlled laboratory setup that immersed users in the task of configuring a desktop computer by making installation decisions about various software applications. Each of the programs contained secondary features that presented the user with various trade-offs. Users had to balance their interest in potentially desirable features (e.g., screen saver) with privacy, security, and performance risks of different magnitudes (e.g., transfer of personally identifying information) that were disclosed in the either EULA notices or EULA notices in combination with either short notices or generic warnings. We found that users are often willing to install programs with potentially harmful behaviors in exchange for access to software programs with desirable features. Users were generally unaware of the potentially negative secondary aspects of the programs they installed and did not read the EULA or ToS notices. When informed in a post-study interview of the EULA's contents participants often regretted their decision to install programs and indicated a desire to undo their actions.

In the next step we introduced two additional information conditions (Microsoft SP2 warning and Short Notice) to improve users' knowledge and understanding of the EULA terms. Surprisingly, we did not find a behavioral change in the number of programs installed. Even users that carefully read the Short Notice statements were often willing to proceed with the installation of potentially harmful programs.

In the Short Notice condition, however, users felt better informed, evinced greater understanding of potential risks of the software during the post-study interview, and had a better understanding of the EULA contents and, therefore, program functionality.

We suggest that the improved awareness and reduced regret indicate that Short Notices move toward a more meaningful notice and consent experience. However, we strongly believe that mutual assent, in the legal sense, is largely unachievable given the current state of notices and law.

Our data suggests that providing for comparison shopping among programs with similar primary features prior to installation, may lead to increased focus and evaluation of secondary features that negatively affect privacy, security, and performance.

HCI approaches that improve notice methods can assist users in controlling their desktop experience, but alone they are insufficient.